

# POLYNOMIAL TIME COMPUTABLE TRIANGULAR ARRAYS FOR ALMOST SURE CONVERGENCE

VLADIMIR DOBRIĆ<sup>†</sup>, MARINA SKYERS, AND LEE J. STANLEY

ABSTRACT. For  $x \in (0, 1)$ , write  $x = \sum_{i=1}^{\infty} \varepsilon_i(x)2^{-i}$ , with each  $\varepsilon_i(x) \in \{0, 1\}$  and  $\varepsilon_i(x) = 0$  for infinitely many  $i$ . Let  $R_i(x) := (-1)^{1+\varepsilon_i(x)}$  and  $\{S_n\}$  be the random walk on  $\mathbb{Z}$  defined on  $(0, 1) : S_n = \sum_{i=1}^n R_i$ . By the Central Limit Theorem, the sequence  $\{S_n/\sqrt{n}\}$  converges weakly to the standard normal distribution on  $(0, 1)$ . It is well known that there are  $S_n^*$ , equal in distribution to  $S_n$ , for which Skorokhod showed that  $\{S_n^*/\sqrt{n}\}$  converges almost surely to the standard normal on  $(0, 1)$ .

We introduce a general method for constructing from  $\{R_i\}$  triangular array representations  $(R_{n,i}^* | 1 \leq i \leq n, n \in \mathbb{Z}^+)$  of  $\{S_n^*\}$ , where each  $R_{n,i}^*$  is a mean 0, variance 1 Rademacher random variable depending only on the first  $n$  bits of the binary expansion of  $x \in (0, 1)$ . These representations are *strong* in that for each  $n$ ,  $S_n^*$  is equal to the sum of the i.i.d family,  $(R_{n,i}^* | 1 \leq i \leq n)$ , pointwise, as a function on  $(0, 1)$ , not just in distribution. Our construction method gives a bijection between the set of all representations with these properties and the set of sequences,  $\{\pi_n\}$ , where each  $\pi_n$  is a permutation of  $\{0, \dots, 2^n - 1\}$  with the property that we call *admissibility*.

We show that the complexity of any sequence of admissible permutations is bounded below by the complexity of  $2^n$ , the exponential function on natural numbers with base 2. We explicitly construct three such sequences which are polynomial time computable and whose complexity is bounded above by the complexity of the function we denote by SBC (for sum of binomial coefficients), closely related to the binomial distributions with parameter  $p = 1/2$ . We also initiate the study of some additional fine properties of admissible permutations.

## 1. INTRODUCTION

1.1. **Motivation.** Let  $\{R_i | i \in \mathbb{Z}^+\}$  be an i.i.d sequence of random variables, each with mean 0 and variance 1, and for each  $n > 0$ , let  $S_n = \sum_{i=1}^n R_i$  be the  $n^{\text{th}}$  partial sum; thus, by the classical Central Limit Theorem, the sequence  $\{S_n/\sqrt{n}\}$  converges weakly to the standard normal. It is well known, [11], that there is another sequence,  $\{S_n^*\}$ , defined on  $(0, 1)$  (equipped with Lebesgue measure), with each  $S_n^*$  equivalent in distribution to  $S_n$ , such that  $\{S_n^*/\sqrt{n}\}$  converges almost surely to  $Z$ , the standard normal. However, is there a general method for obtaining, for each  $n$ , an i.i.d. family  $(R_{n,i}^* | 1 \leq i \leq n)$ , with each  $R_{n,i}^*$  equal in distribution to  $R_i$ , and whose sum is equal (literally, pointwise, not just in distribution) to  $S_n^*$ ? Once such families are obtained, they provide a *strong* triangular array representation of  $\{S_n^*\}$ . This is the natural counterpart, for almost sure convergence, of the standard notion of triangular array representation.

At this level of generality, the problem appears to be quite difficult. This paper begins the investigation of the problem in the simple but important setting where the sequence  $\{S_n\}$  is the

*Date:* 8 March, 2016.

2010 *Mathematics Subject Classification.* Primary 60G50, 60F15 ; Secondary 68Q15, 68Q17, 68Q25.

*Key words and phrases.* Central Limit Theorem, Almost Sure Convergence, Strong Triangular Array Representations, Admissible Permutations, Polynomial Time Computability, Sums of Binomial Coefficients.

Skyers and Stanley dedicate this paper to the memory of our dear departed friend and co-author, Vladimir Dobrić. The important contribution of S. Buss will be explicitly acknowledged at various points in the body of the paper. We would also like to thank P. Clote and A. Nerode for helpful discussions of complexity issues, and to thank Nerode for pushing us to improve our upper complexity bounds and suggesting the connection between tameness and continuity. We are indebted to our Lehigh colleagues, Vince Coll, Daniel Conus, Rob Neel and Joe Yukich for many helpful comments and suggestions.

(equiprobable) random walk on  $\mathbb{Z}$  with domain  $(0, 1)$ . For  $0 < x < 1$ , write  $x = \sum_{i=1}^{\infty} \varepsilon_i(x) 2^{-i}$ , with each  $\varepsilon_i(x) \in \{0, 1\}$  and  $\varepsilon_i(x) = 0$  for infinitely many  $i$ . For  $1 \leq i \leq n$  and  $0 < x < 1$ , we take  $R_i(x) = (-1)^{1+\varepsilon_i(x)}$ ; this gives the simplest expression for the  $S_n$ . Even in this simple setting, the behavior of the  $S_n/\sqrt{n}$  is extremely chaotic and the disorder increases with  $n$ . One manifestation of this chaos is an easy consequence of the LIL, [7], [8] for example: for almost all  $x$ ,  $\overline{\lim}_{n \rightarrow \infty} S_n(x)/\sqrt{n} = \infty$  and  $\underline{\lim}_{n \rightarrow \infty} S_n(x)/\sqrt{n} = -\infty$ . On the other hand, each  $S_n^*$  is a non-decreasing step function, mirroring the almost sure convergence of the sequence of normalizations.

The graphs of  $S_n$  and  $S_n^*$  for  $n = 6, 7$  are included below.  $S_n$  is shown in magenta, while  $S_n^*$  is shown in green.

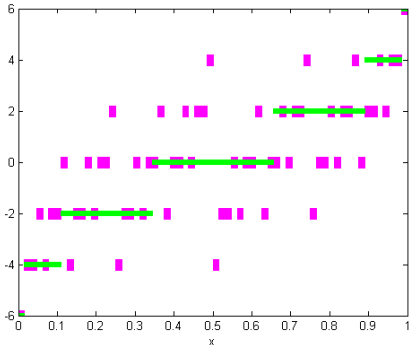


FIGURE 1.  $S_6, S_6^*$

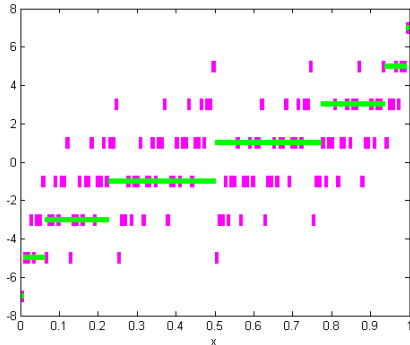


FIGURE 2.  $S_7, S_7^*$

Since  $S_n^*$  is equal in distribution to  $S_n$ , it follows that  $S_n^*$  does have triangular array representations. But what about *strong* ones, in the sense of the first paragraph? Specializing to this setting, the problem laid out in that paragraph can be restated as follows.

**Question 1.** *How do we obtain strong triangular array representations,  $(R_{n,i}^* | n \in \mathbb{Z}^+, 1 \leq i \leq n)$ , of  $\{S_n^*\}$ ? What do the  $R_{n,i}^*$  look like, as functions of  $x$ ?*

The LIL has implications, here, as well. For example, for each  $n$ , at least one of the  $R_{n,i}^*$  must depend on more than one bit. Also, the  $R_{n,i}^*$  must depend on  $n$ , not just on  $i$ .

We will give an explicit procedure for obtaining the sought-after  $R_{n,i}^*$ , and they will have an additional property; they are *trim* in that, for fixed  $n$ , each  $R_{n,i}^*(x)$  will depend only on  $(\varepsilon_1(x), \dots, \varepsilon_n(x))$ . This leads naturally to the next question.

**Question 2.** *What are the trim, strong triangular array representations of  $\{S_n^*\}$ ?*

Our procedure starts from any sequence  $\{\pi_n\}$ , where each  $\pi_n$  is a permutation of  $\{0, \dots, 2^n - 1\}$  with the additional property of being *admissible*. Any permutation,  $\pi$ , of  $\{0, \dots, 2^n - 1\}$ , can be viewed as permuting the level  $n$  dyadic intervals (by permuting their indices). This provides a rearrangement of  $(0, 1)$ . Such a permutation is *admissible* iff  $S_n^*$  results when the corresponding rearrangement is followed by applying  $S_n$  (as a function). This is made precise in Equation (1) of subsection (1.2).

For each  $n$ , the passage from  $\pi_n$  to  $(R_{n,i}^* | 1 \leq i \leq n)$  is explicit, canonical and one-to-one and is given by Equation (2) of the proof of Theorem 1 in (2.2). Further, as  $\pi_n$  varies over admissible permutations, our procedure generates *all* possible suitable families  $(R_{n,i}^* | 1 \leq i \leq n)$ , where each  $R_{n,i}^*$  is trim. The passage from  $(R_{n,i}^* | 1 \leq i \leq n)$  to  $\pi_n$  is given by Equation (3), also in (2.2). The obvious extension to a canonical bijection between sequences of admissible permutations and trim strong triangular array representations of  $\{S_n^*\}$  is given by Corollary 1. Thus Theorem 1 and Corollary 1 answer Questions 1 and 2.

Since almost sure convergence is such a restrictive condition, it is natural to ask how hard it is to produce the trim strong triangular array representations of  $\{S_n^*\}$  and what additional special

properties they must have. As with the existence of trim strong triangular array representations, prior to this paper, very little was known; to our knowledge, the questions in the previous sentence have not been considered until now. Once we know how to associate sequences of admissible permutations to trim strong triangular array representations, it becomes natural to pursue these questions in terms of the complexity of the associated sequences. The second half of the paper carries out such a complexity analysis, motivated by the following questions.

**Question 3.** *Are there trim, strong triangular representations of  $\{S_n^*\}$  of low complexity?*

**Question 4.** *Are there trim, strong triangular array representations of  $\{S_n^*\}$  which differ as little as possible from the above representation of  $\{S_n\}$  and which are also of low complexity?*

We explicitly construct three trim, strong triangular array representations of quite low complexity, as measured by the complexity of their classifying sequences of admissible permutations,  $\{F_n\}$ ,  $\{G_n\}$  and  $\{H_n\}$ . Our basic complexity estimate is that they are all polynomial time computable (we make this precise in subsection (1.2)). This is the content of Theorem 2, in subsection (3.4), for  $\{F_n\}$  and of Theorem 3, in subsection (4.2), for  $\{G_n\}$  and  $\{H_n\}$ . These results therefore answer Question 3 affirmatively. Since  $\{G_n\}$  and  $\{H_n\}$  are constructed so as to differ as little as possible from the representation of  $\{S_n\}$  by  $\{R_i\}$ , Theorem 3 answers Question 4 affirmatively.

The proofs of Theorems 2 and 3 yield the somewhat sharper result that each of  $\{F_n\}$ ,  $\{G_n\}$  and  $\{H_n\}$  is very simply computed in terms of the function we denote by SBC (for Sum of Binomial Coefficients) introduced in Definition 1 in subsection (3.1). This function is very naturally associated with the binomial distributions with parameter  $p = 1/2$ . The computation of each of the three sequences in terms of SBC is a counterpart to the result that  $2^n$  has a very simple expression in terms of *any* sequence,  $\{\pi_n\}$ , of admissible permutations. Thus, the complexity of each of  $\{F_n\}$ ,  $\{G_n\}$  and  $\{H_n\}$  is bracketed in the fairly narrow range between that of  $2^n$  and that of SBC. We shed further light on the relationship between SBC and  $\{F_n\}$  in Corollary 4 of subsection (3.5); discussion is deferred until (1.3.5) and Section 3.

While their properties are indeed rather special, the trim strong triangular array representations corresponding to  $\{F_n\}$ ,  $\{G_n\}$  and  $\{H_n\}$  are, perhaps surprisingly, not so difficult to produce, since they are of low complexity. At least in this context, the “cost” of the passage from  $\{R_i/\sqrt{n}\}$  and the weakly convergent  $\{S_n/\sqrt{n}\}$  to the (trim) strong triangular array representations of the almost surely convergent  $\{S_n^*/\sqrt{n}\}$  turns out to be surprisingly modest. Progress has been made in the direction of extending our methods to a more general setting. This will be the subject of a planned sequel to this paper.

This paper grows out of Chapters 3 and 4 of Skyers’ dissertation, [12], written with Stanley as advisor. Dobrić, served as a “co-advisor”, and provided the inspiration and impetus for the entire project. For recent work related to Skorokhod’s work, in a rather different vein than this paper, see [2], [3].

**1.2. Preliminaries, Notation, Conventions.** Let  $X$  be a random variable (on *any* probability space). Let  $F_X$  be the cumulative distribution of  $X$ . By the *quantile of  $X$*  (denoted by  $X^*$ ), we mean the random variable on  $(0, 1)$  (equipped with Lebesgue measure,  $\lambda$ , on Borel sets,  $\mathcal{B}$ ) defined by:

$$X^*(x) := \inf\{t \in \mathbb{R} | F_X(t) \geq x\}.$$

It is well-known that  $X$  and  $X^*$  are equal in distribution. Skorokhod, [11], showed that if  $\{X_n\}$  is a sequence of random variables (on *any* probability space) converging weakly to  $X$ , then the sequence of quantiles,  $X_n^*$ , converges almost surely to  $X^*$ .

In order to compare the structure of the initial sequence to that of the sequence of quantiles, the probability space of the  $X_n$  should be  $((0, 1), \mathcal{B}, \lambda)$ , as above. In what follows, we work exclusively in this probability space.

In this paper,  $i, j, k, m, n$  will *always* denote non-negative integers (elements of  $\mathbb{N}$ ). Most often, we will have  $n > 0$ . We use  $|X|$  for the cardinality of a set,  $X$ . To emphasize that a union is a *disjoint union* we use  $\sqcup$  or  $\sqcup$  rather than the usual  $\cup$  or  $\cup$ . When the nature of the index set is

clear or has been established, we use  $\{a_i\}$  to denote the sequence (possibly finite, possibly multi-indexed) whose term, for index  $i$ , is  $a_i$ . We use  $\chi_{Y,U}$  to denote the characteristic (or indicator) function of a set  $Y$ , viewed as a subset of an ambient set  $U$ , the domain of the characteristic function. When  $U$  is clear from context, we will omit it in the subscript. This notation is intended to cover the situation where  $Y$  is a relation, i.e. where  $U$  is a set of  $d$ -tuples for some fixed  $d > 1$ .

For integers,  $n > 0$ , and  $0 \leq k < 2^n$ ,  $D_{n,k}$  denotes the  $k^{\text{th}}$  level  $n$  dyadic interval:

$$D_{n,0} = (0, 2^{-n}), \text{ and for } 0 < k < 2^n, D_{n,k} = [2^{-n}k, 2^{-n}(k+1)).$$

Note that both  $S_n$  and  $S_n^*$  are constant on each level  $n$  dyadic interval. A permutation,  $\pi$ , of  $\{0, 1, \dots, 2^n - 1\}$  is *admissible* if

$$(1) \quad \text{for all } k \in \{0, 1, \dots, 2^n - 1\}, \text{ all } x \in D_{n,k} \text{ and all } y \in D_{n,\pi(k)}, S_n^*(x) = S_n(y).$$

In several places, we will have a function,  $\phi$ , with domain  $(0, 1)$ , which, for some  $n$ , is constant on each of the  $D_{n,k}$ . We then use  $I\phi$  (“I $\phi$ ” for the integer version of  $\phi$ ) to denote the function with domain  $\{0, \dots, 2^n - 1\}$ , whose value at  $k$  is the constant value of  $\phi$  on  $D_{n,k}$ . Thus, for example,  $IS_n$  and  $IS_n^*$  will denote the integer versions of  $S_n$  and  $S_n^*$ , respectively.

We adopt a similar convention for subsets,  $X \subseteq (0, 1)$ , such that  $X$  is a union of level  $n$  dyadic intervals. We will then use  $IX$  to denote the set of  $k$  such that  $D_{n,k} \subseteq X$ . Strictly speaking, in both cases (function or subset) the dependence on the specific  $n$  involved should be part of the notation, but, in all instances, this will already be incorporated into the notation used for the specific  $\phi$  or  $X$  involved.

Our basic complexity estimate is in terms of polynomial time computability. This notion is robust across different detailed models of computations, each of which has its own sensible notion of “elementary operation”. Accordingly, as is customary, we omit a detailed development of what is involved in this notion.

If  $f$  is a function of  $d$  natural number arguments,  $f$  is polynomial time computable (P-TIME) iff for some polynomial,  $p(n)$ , the value of  $f$  can be computed in at most  $p(n)$  elementary operations whenever all arguments are smaller than  $2^n$ . This is consistent with the usual treatments (e.g. [4] or [10]), which, for the most part, treat arguments and values as bitstrings or vectors of bitstrings, rather than in terms of the encoded natural numbers. In some important instances,  $f$  will have  $1 + d$  arguments, the first of which is viewed as being  $n$  itself (the argument of  $p$ .) In this context, the requirement is that at most  $p(n)$  elementary operations are required to compute  $f(n, x_1, \dots, x_d)$  whenever each  $x_i < 2^n$ . Polynomial-time decidable (P-TIME decidable) relations are ones whose characteristic functions are P-TIME.

**1.3. Summary and Further Discussion of Results.** By Corollary 1, the existence of trim strong triangular array representations of  $\{S_n^*\}$  reduces to the existence of sequences of admissible permutations, which further reduces to the existence of admissible permutations of  $\{0, \dots, 2^n - 1\}$ , for each  $n$ . This is established in part 2 of Lemma 1 of (3.1); the precise statement is that there are  $\prod_{i=0}^n \binom{n}{i}!$  of them. This count builds on a more concrete characterization of admissibility developed, among other things, in (3.1).

In (3.2), Corollary 2 pulls together the statements of Theorem 1, Corollary 1 and part 2 of Lemma 1 to give the existence proof for trim strong triangular array representations of  $\{S_n^*\}$ . Proposition 1 builds on Corollary 2 by constructing a strong but non-trim triangular array representation starting from a trim strong one. Proposition 2, which also builds on some of the material from (3.1), is a “non-persistence” result in that it shows that in any sequence  $\{\pi_n\}$  of admissible permutations,  $\pi_n$  never persists to be a subfunction of  $\pi_{n+1}$ , and that in any trim strong triangular array representation  $(R_{n,i}^* | n > 0, 1 \leq i \leq n)$  of  $\{S_n^*\}$ , for any  $n > 0$ , it is never possible for all of the  $R_{n,i}^*$  to persist to be the corresponding  $R_{n+1,i}^*$ . This provides another proof of the second consequence of the LIL mentioned following Question 1 in (1.1) and highlights some important ways in which the trim strong triangular array representations of  $\{S_n^*\}$  must differ from the simple representation  $\{R_i\}$  of  $\{S_n\}$ .

1.3.1. *The role of trimness.* Proposition 1 shows that trimness does not “come for free”. Given that there can be no strong triangular array representation for  $\{S_n^*\}$  in which each  $R_{n,i}^*$  depends on only one bit, trimness is a natural “next best hope”. Its central role in Theorem 1 and Corollary 1 is further evidence for its naturality, as is the following equivalent characterization of trimness, suggested by A. Nerode.

Let  $V_n$  be  $\{-1, 1\}^n$ . Let  $\mathcal{V}$  be the topological product of the  $V_n$  equipped with the discrete topologies and let  $V$  be the set of points of  $\mathcal{V}$ . Suppose that for  $n \geq i$ ,  $R'_{n,i}$  is a Rademacher random variable on  $(0, 1)$  (we are not necessarily assuming, yet, that  $\{R'_{n,i}\}$  is a triangular array nor that it represents  $\{S_n^*\}$ ). This provides us with a transformation,  $T$ , from  $(0, 1)$  to  $V$ , by taking  $T(x)_n := (R'_{n,1}(x), \dots, R'_{n,n}(x))$ . It is then clear that the condition:

$$\text{for all } i \leq n, R'_{n,i} \text{ depends at most on } \varepsilon_1, \dots, \varepsilon_n$$

is equivalent to the condition:

$$\text{the associated transformation } T \text{ is Lipschitz-continuous with } \delta = \epsilon.$$

Then, specializing to the situation where the  $R'_{n,i}$  do furnish a strong triangular array representation of  $\{S_n^*\}$ , the second displayed formula provides our equivalent characterization of trimness. We are grateful to A. Nerode for suggesting that we seek this type of characterization, and for the observation that the transformation  $T$  can be feasibly implemented, since the implementation would satisfy a strong form of bounded memory; this is an equivalent reformulation of the Lipschitz continuity.

1.3.2. *Transition to Complexity:  $2^n$  is a lower bound.* In (3.3) we introduce the natural encoding,  $\Pi$  of a sequence,  $\{\Pi_n\}$ , of admissible permutations, and explicitly begin to deal with complexity issues. It is here that we really begin to exploit the “toolkit” material developed in (3.1). We prove Proposition 3, which establishes that the exponential function,  $2^n$ , is a lower bound for the complexity of *any* such sequence  $\{\Pi_n\}$ . Our approach to this, and to related questions, will be briefly outlined in (1.3.5), below and more fully discussed at the start of Section 3.

1.3.3. *Preview of Theorem 2.* While Corollary 2 settles the question of the existence of trim strong triangular array representations of  $\{S_n^*\}$ , in Definition 4 ((3.4)) we explicitly construct the sequence  $\{F_n\}$  of admissible permutations. Building on Proposition 4 and Corollary 3, Theorem 2 answers Question 3 affirmatively by establishing that  $F$ , the natural encoding of this sequence, is P-TIME and can be simply computed in terms of SBC. We also give an even cleaner and simpler defining expression for  $2^n$  in terms of  $F$ , improving slightly on the proof of Proposition 3. The discussion of Corollary 4, proved in (3.5), is deferred until (1.3.5) and Section 3.

1.3.4. *Preview of Theorem 3.* The affirmative answer to Question 4 is provided by Theorem 3, proved in (4.2). In (4.1), culminating in Definition 7, we construct  $\{G_n\}$ , a variant of the sequence,  $\{F_n\}$ . Among admissible permutations of  $\{0, \dots, 2^n - 1\}$ ,  $G_n$  is maximal for agreement with the identity function. Thus, the extent to which trim strong triangular array representations of  $\{S_n^*\}$  *must* differ from the canonical representation of  $\{S_n\}$  is measured by the extent to which the  $G_n$  differ from the identity permutations.

The construction of  $\{G_n\}$  is also motivated by a rather different notion of complexity: that of an individual admissible permutation. This also motivates the construction of  $\{H_n\}$ , the other variant of  $\{F_n\}$  (Definition 11 of (4.1)). We impose additional natural properties on the  $G_n$  and  $H_n$  to guarantee that their orbit structures will be simpler than the orbit structures of the  $F_n$ . While Remark 6 and Definition 7 immediately make it clear that each  $G_n$  is admissible, this is a more substantial issue for the  $H_n$  and is established in Proposition 5 of (4.1), the analogue for  $\{H_n\}$  of Remark 6.

The analogue of Theorem 2 for the natural encodings,  $G$ , of  $\{G_n\}$ , and  $H$ , of  $\{H_n\}$  is provided by Theorem 3. The expression for  $2^n$  in terms of  $G$  is fairly close to the one in terms of  $F$ , but for  $H$ , we content ourselves with the general lower bound statement of Proposition 3. This difference between  $F$  and  $G$ , on the one hand, and  $H$ , on the other, is foreshadowed by the discussion at

the end of (3.5), and revisited at the end of (4.1). Similar issues, also discussed at the end of (4.1), are obstacles to obtaining a genuine analogue of Corollary 4 for  $G$  or  $H$ . The proof that each of  $G$  and  $H$  is P-TIME and is simply and explicitly computed in terms of SBC proceeds by analogy to Theorem 2, and follows the general approach sketched in (1.3.5). This builds on Proposition 6, which plays the role of the combination of Proposition 4 and Corollary 3.

1.3.5. *Complexity Issues.* For the lower bounds, established by Equation (6) of Proposition 3, Equation (8) of Theorem 2, and Equation (13) of Theorem 3, the approach is to express  $2^n$  explicitly and uniformly in  $n$ , using the sum of at most  $n$  values (including repeated values) of the function involved. All of the corresponding arguments are obtained from  $n$ , very simply, explicitly, and uniformly in  $n$ . In Equation (6), there are  $n$  distinct values involved, and the sum of these values is incremented by 1 to obtain  $2^n$ . In Equation (8), for  $F$ , there is just one value, repeated twice. Finally, for Equation (13), for  $G$ , there is also just one value, repeated twice, but that value is the maximum of two values. In both of the latter cases,  $2^n$  is simply the sum of the repeated values (i.e., twice the repeated value, but the point is to do things using only addition and no multiplication).

The proofs that  $F$ ,  $G$  and  $H$  are P-TIME have a common structure, though the cases in the definitions of  $G$ ,  $H$  result in technical complications, especially for  $H$ . Here, accordingly, it is only for  $F$  (Theorem 2) that we will outline the main ideas of the proof.

In subsections (3.1) and (3.4), we introduce the function SBC (in Definition 1) and a number of other auxiliary functions and relations, notably the two functions, IStep and EW. The function IStep computes “positions” with respect to SBC and is introduced in the comments following Remark 1, in (3.1). We introduce EW in Definition 5 of (3.4). It is the enumerating function for Weight (Definition 2: the usual Hamming weight of a positive integer). The sequence <http://oeis.org>, 2010, Sequence A066884, [9], encodes EW. IStep bears the same relationship to  $\{S_n^*\}$  as Weight does to  $\{S_n\}$ .

In subsection (3.4), Proposition 4 establishes, among other things, that for all  $n$  and all  $i \leq n$  the computation of  $SBC(n, i)$  can be carried out using  $O(n^2)$  additions of integers all below  $2^n$ , with all of the intermediate sums being less than  $2^n$ . This guarantees that the function IStep is P-TIME.

The corresponding result for the function EW is given by Corollary 3 which also establishes that the relation expressed by Equation (7) is P-TIME decidable. Corollary 3 is the culmination of a sequence of results (Proposition 4, Lemmas 2 and 3) where the notion of “tame” relation, introduced in Definition 3, is a key ingredient. Lemma 2 establishes that the enumerating function (viz. Definition 3) for a tame relation is P-TIME. Lemma 3 establishes the tameness of the relation whose enumerating function is EW (and thus, with Lemma 2, that EW is P-TIME). It follows from the proof of Lemma 3 that EW itself can be simply computed in terms of SBC and that solutions,  $m$ , of Equation 7 can be computed in polynomial time as functions of  $n$  and  $k$ .

The proof of Theorem 2 then proceeds by showing that for  $n > 0$  and  $k < 2^n$ ,  $F(n, k) = m < 2^n$  is the unique solution of Equation (7). We are very grateful to S. Buss who provided invaluable assistance on several occasions. In particular, he confirmed the validity of our approach to Proposition 4, pointed out the references given there and supplied a very nice argument that evolved into the proof of Lemma 3. He also suggested combining these ideas with binary search (a variant of the Bisection Algorithm). In the course of working out the details, we isolated the notion of tameness and formulated and proved Lemma 2. A bit more detail on the material of this subsection is given in the overview of Section 3.

## 2. THEOREM 1 AND COROLLARY 1

2.1. **Preliminaries for Theorem 1.** For  $x \in (0, 1)$ , we set:

$$\mathbf{r}_n(x) := (\varepsilon_1(x), \dots, \varepsilon_n(x)),$$

$$\mathbf{s}_n(x) := \left( (-1)^{1+\varepsilon_1(x)}, \dots, (-1)^{1+\varepsilon_n(x)} \right).$$

On  $D_{n,k}$ ,  $\mathbf{r}_n(x), \mathbf{s}_n(x)$  are constant. Therefore, following the convention in the final paragraph of (1.3), we denote these constant values by  $\mathbf{I}\mathbf{r}_n(k), \mathbf{I}\mathbf{s}_n(k)$ , respectively.

Note that  $\mathbf{I}\mathbf{r}_n(k)$  does NOT denote the  $k$ th component of a vector,  $\mathbf{I}\mathbf{r}_n$ , rather it denotes the vector (a length  $n$  bitstring) itself. We will denote the  $i^{\text{th}}$  component of this vector by  $(\mathbf{I}\mathbf{r}_n(k))_i$ . Note that this is just  $\varepsilon_i(x)$  for any  $x \in D_{n,k}$ . Similar observations hold with  $\mathbf{s}$  in place of  $\mathbf{r}$  (and  $\{-1, 1\}$  replacing  $\{0, 1\}$ ).

Note, further, that  $\mathbf{I}\mathbf{r}_n(k)$  is the reversal of the binary representation of  $k$ :  $k = \sum_{i=1}^n 2^{n+1-i} (\mathbf{I}\mathbf{r}_n(k))_i$ , and that  $(\mathbf{I}\mathbf{r}_n(k) | k < 2^n)$  enumerates  $\{0, 1\}^n$  in increasing order with respect to the lexicographic ordering. For  $\mathbf{r} \in \{0, 1\}^n$ , we also let:

$$D_{\mathbf{r}} := \{x \in (0, 1) | \mathbf{r}_n(x) = \mathbf{r}\}.$$

Letting  $k$  be such that  $\mathbf{r} = \mathbf{I}\mathbf{r}_n(k)$ , we note that  $D_{\mathbf{r}} = D_{n,k} = \{x \in (0, 1) | \mathbf{r}_n(x) = \mathbf{I}\mathbf{r}_n(k)\}$ .

We use  $\nu_n$  to denote the order isomorphism (with respect to lexicographic order) between  $\{0, 1\}^n$  and  $\{-1, 1\}^n$ , thus for  $\mathbf{r} \in \{0, 1\}^n$  and  $1 \leq i \leq n$ ,  $(\nu_n(\mathbf{r}))_i = (-1)^{1+(\mathbf{r})_i}$ . Note that  $\mathbf{I}\mathbf{s}_n(k) = \nu_n(\mathbf{I}\mathbf{r}_n(k))$ . It is also worth noting that *any* permutation,  $\pi$ , of  $\{0, \dots, 2^n - 1\}$  is naturally viewed as a permutation of  $\{0, 1\}^n$ , by taking  $\pi(\mathbf{I}\mathbf{r}_n(k))$  as defined to be  $\mathbf{I}\mathbf{r}_n(\pi(k))$ , and similarly with  $\{-1, 1\}$  replacing  $\{0, 1\}$  and  $\mathbf{s}$  replacing  $\mathbf{r}$ .

## 2.2. Theorem 1 and Corollary 1.

**Theorem 1.** *For each  $n$ , there is a canonical bijection between admissible permutations of  $\{0, \dots, 2^n - 1\}$  and representations of  $S_n^*$  as a sum*

$$S_n^* = \sum_{i=1}^n R_{n,i}^*,$$

where  $(R_{n,i}^* | 1 \leq i \leq n)$  is an i.i.d. family of Rademacher random variables each of which has mean 0, variance 1 and depends only on  $\mathbf{r}_n$ .

*Proof.* Fix  $n > 0$ . We first construct the  $R_{n,i}^*$ , given  $\pi$ , and then construct  $\pi$  given the  $R_{n,i}^*$ . We then carry out the necessary verifications in each direction.

First, let  $\pi$  be an admissible permutation of  $\{0, \dots, 2^n - 1\}$ . For  $x \in (0, 1)$ , let  $k$  be such that  $x \in D_{n,k}$ , and let  $1 \leq i \leq n$ . Then:

$$(2) \quad \text{let } y \text{ be any member of } D_{n,\pi(k)} \text{ and define: } R_{n,i}^*(x) := (-1)^{1+\varepsilon_i(y)}.$$

Conversely, given an independent family,  $(R_{n,i}^* | 1 \leq i \leq n)$ , such that  $S_n^* = \sum_{i=1}^n R_{n,i}^*$ , where each  $R_{n,i}^*$  is Rademacher with mean 0 and variance 1 and depends only on  $\mathbf{r}_n(x)$ , we obtain  $\pi$  as follows. Given  $k < 2^n$ , let  $x \in D_{n,k}$ , let  $\mathbf{s} = (R_{n,i}^*(x) | 1 \leq i \leq n)$  and define:

$$(3) \quad \pi(k) = \text{that } m < 2^n \text{ such that } \mathbf{s} = \mathbf{I}\mathbf{s}_n(m).$$

Clearly these constructions yield a bijection, so we turn to the necessary verifications.

First suppose  $\pi$  is admissible and that the  $R_{n,i}^*$  are defined by Equation (2). Clearly these  $R_{n,i}^*$  depend only on  $\mathbf{r}_n(x)$ . In order to see that they sum to  $S_n^*$ , note that:

$$\text{for all } k < 2^n \text{ and all } x \in D_{n,k}, S_n^*(x) = S_n(y), \text{ for any } y \in D_{n,\pi(k)},$$

$$\text{i.e. } S_n^*(x) = \sum_{i=1}^n (-1)^{1+\varepsilon_i(y)}, \text{ for any such } y, \text{ i.e. } S_n^*(x) = \sum_{i=1}^n R_{n,i}^*(x); \text{ this suffices.}$$

To see that each  $R_{n,i}^*$  is Rademacher with mean 0 and variance 1, fix  $i$  and  $\epsilon \in \{0, 1\}$  and let  $A := \{\mathbf{t} \in \{0, 1\}^n | t_i = \epsilon\}$ ; then  $|A| = 2^{n-1}$ . Since  $\pi$  is 1-1,  $|\pi^{-1}[A]| = 2^{n-1}$ . Now, viewing  $\pi$  as a permutation of  $\{0, 1\}^n$ , we have that:

$$\pi^{-1}[A] = \{\mathbf{r} \in \{0, 1\}^n | (\pi(\mathbf{r}))_i = \epsilon\} \text{ and } \{x | (\pi(\mathbf{r}_n(x)))_i = \epsilon\} = \bigsqcup_{\mathbf{r} \in \pi^{-1}[A]} D_{\mathbf{r}}.$$

It follows that:

$$\lambda(\{x | (\pi(\mathbf{r}_n(x)))_i = \epsilon\}) = \lambda\left(\bigsqcup_{\mathbf{r} \in \pi^{-1}[A]} D_{\mathbf{r}}\right) = 2^{n-1} \cdot 2^{-n} = 1/2; \text{ this suffices.}$$

In order to see that these  $R_{n,i}^*$  are independent, it suffices to show that:

$$\text{for all } \mathbf{s} = (s_1, \dots, s_n) \in \{-1, 1\}^n, p(s_1, \dots, s_n) = p_1(s_1) \cdot \dots \cdot p_n(s_n),$$

where  $p$  is the joint pmf of the  $R_{n,i}^*$  and  $p_i$  is the pmf of  $R_{n,i}^*$  alone. We showed that  $p_1(s_1) \cdot \dots \cdot p_n(s_n) = 2^{-n}$ , so, again viewing  $\pi$  as a permutation of  $\{0, 1\}^n$ , let  $\mathbf{r} := \pi^{-1} \circ (\nu_n)^{-1}(\mathbf{s})$  and note that:

$$P(R_{n,1}^* = s_1, \dots, R_{n,n}^* = s_n) = \lambda(\{x | \pi(\mathbf{r}_n(x)) = \nu_n^{-1}(\mathbf{s})\}) = \lambda(D_{\mathbf{r}}) = 2^{-n}.$$

For the opposite direction, suppose that  $(R_{n,i}^* | 1 \leq i \leq n)$  is given with the stated properties. Let  $\pi$  be defined by Equation (3). We first show that  $\pi$  is one-to-one. For this, let  $x \in D_{n,k}$ ,  $\mathbf{s} = (R_{n,i}^*(x) | 1 \leq i \leq n)$  and note that if  $\mathbf{u} \in \{0, 1\}^n$  is such that

$$\text{for } y \in D_{\mathbf{u}}, (R_{n,i}^*(y) | 1 \leq i \leq n) = \mathbf{s}, \text{ then } \mathbf{u} = \mathbf{I}r_n(k).$$

If this were to fail we would have that

$$P(R_{n,1}^* = s_1, \dots, R_{n,n}^* = s_n) \geq \lambda(D_{\mathbf{u}}) + \lambda(D_{\mathbf{I}r_n(k)}) = 2^{-n+1},$$

which contradicts our hypotheses on the  $R_{n,i}^*$ . Thus,  $f$  is one-to-one. Admissibility then follows, because now, by hypothesis, if  $x \in D_{n,k}$  and  $m = \pi(k)$ , then:

$$S_n^*(x) = \sum_{i=1}^n R_{n,i}^*(x) = \sum_{i=1}^n s_i, \text{ but also for any } y \in D_{n,m}, S_n(y) = \sum_{i=1}^n s_i,$$

as required.  $\square$

**Corollary 1.** *There is a canonical bijection between sequences,  $\{\pi_n\}$ , of admissible permutations of  $\{0, \dots, 2^n - 1\}$  and trim, strong triangular arrays for  $\{S_n^*\}$ .*  $\square$

Given  $n$  and  $(R_{n,i}^* | 1 \leq i \leq n)$ , Equation (3) is best seen as as a finer version of Equation (1) (the definition of admissible permutation). Incorporating the additional information in the representations  $(R_i | 1 \leq i \leq n)$  and  $(R_{n,i}^* | 1 \leq i \leq n)$  singles out a specific admissible permutation, whereas Equation (1) defines the set of all of them. Equation (2) reverses this, taking as given the canonical representation,  $(R_i | 1 \leq i \leq n)$ , together with a specific admissible permutation and singling out a specific representation,  $(R_{n,i}^* | 1 \leq i \leq n)$ , of  $S_n^*$ .

### 3. THE ROAD TO THEOREM 2

In (3.1) we introduce the notions that will provide the “toolkit” for the rest of the paper, and, in particular for Theorems 2 and 3. In Definition 1, we introduce the functions  $\text{Step}_n$ ,  $\text{Weight}_n$  and  $\text{SBC}$ . Incorporating Remark 1 then immediately gives us the functions  $\text{IStep}_n$ ,  $\text{IS}$  and  $\text{IS}^*$ . These are the “integer versions” of the functions  $\text{Step}_n$ ,  $S_n$  and  $S_n^*$ , respectively. We also introduce the function  $\text{IStep}$  which is the natural encoding (as a function of two variables) of the family of the  $\text{IStep}_n$ .

In Definition 2, we introduce the sets  $A_{n,i}$  and  $B_{n,i}$  and their “integer versions”  $\text{IA}_{n,i}$  and  $\text{IB}_{n,i}$ . Analogues of these are given in (4.1) in the construction of the  $\{G_n\}$ ,  $\{H_n\}$  and their natural encodings (see (3.3)) by the functions  $G$  and  $H$ .

The  $\text{IA}_{n,i}$  and  $\text{IB}_{n,i}$  are the motivating paradigm for Definition 3, which is particularly important. It is given in abstract form to accommodate five different invocations: one in (3.1) itself, in connection with the  $\text{IA}_{n,i}$ ,  $\text{IB}_{n,i}$ , and the other four in (4.1), in connection with their analogues. The invocation of Definition 3 in (3.1) introduces the three-place relations  $\text{RIA}$  and  $\text{RIB}$ , which encode the families  $\text{IA}_{n,i}$  and  $\text{IB}_{n,i}$  respectively, their associated cardinality functions,  $\text{cd}_{\text{RIA}}$  and  $\text{cd}_{\text{RIB}}$  and enumerating functions,  $\text{ERIA}$  and  $\text{ERIB}$ . The notion of “tameness” is also introduced



in Definition 3; it plays an important role in the complexity analyses carried out in subsections (3.4) and (4.2).

The cardinality functions associated with P-TIME decidable relations form the somewhat unusual complexity class,  $\#P$  (see, e.g., [4], (6.3.5)), which, conjecturally, is not included in the collection of P-TIME functions. In addition to all of the other ways we appeal to tameness, it also guarantees (Item 6. of Remark 3) that the relation itself is P-TIME decidable and that (by definition) its associated cardinality function is P-TIME, allowing us to avoid the issue of  $\#P$ .

We elaborate a bit on the sketch (in (1.3.3) and (1.3.5)) of what is accomplished in subsections (3.4) and (3.5), since the material of subsections (3.2) and (3.3) has already been fully presented in subsection (1.3). In (3.4), Proposition 4 establishes that for all  $n$  and all  $i \leq n$ , the binomial coefficient,  $\binom{n}{i}$  and  $\text{SBC}(n, i)$  can be computed using  $O(n^2)$  additions of integers all below  $2^n$  with all intermediate sums being less than  $2^n$  and so, in particular, in time polynomial in  $n$ . Consequently, the function  $\text{IStep}$  is P-TIME, and the relation  $\text{RIA}$  is tame. This sets the stage for Lemmas 2 and 3, Corollary 3 and Theorem 2. In (3.5), Corollary 4 sheds additional light on the relationship between  $F$  and  $\text{SBC}$  by showing that  $\text{SBC}$  can be simply computed in terms of  $F$  and the function, which we denote by  $\text{Inv}F$ , which is the natural encoding of the sequence  $\{F_n^{-1}\}$ . We conclude (3.5) by arguing for the (informal and therefore necessarily imprecise) thesis that  $\{F_n\}$  is, in fact, is the *simplest* sequence of admissible permutations. The argument appeals to the view of admissible permutations developed at the end of (3.1).

**3.1. Toolkit for Theorems 2 and 3.** As usual,  $F_{B(n,p)}$  denotes the cumulative binomial distribution with parameters  $n, p$ .

**Definition 1.** For  $n > 0$ , set  $\text{SBC}(n, 0) := 0$  and for  $1 \leq i \leq n + 1$ , set

$$\text{SBC}(n, i) := \sum_{j=0}^{i-1} \binom{n}{j}.$$

For  $n > 0$ , and  $x \in (0, 1)$ ,  $\text{Step}_n(x)$  is the unique  $i$  such such that  $F_{B(n,1/2)}(i) \leq x < F_{B(n,1/2)}(i+1)$ . We also set  $\text{Weight}_n(x) := \sum_{i=1}^n \varepsilon_i(x)$ .

*Remark 1.* For  $x \in (0, 1)$ . and  $n > 0$ , the following observations are obvious:

- (1)  $S_n(x) = -n + 2\text{Weight}_n(x)$ ,
- (2)  $\text{Weight}_n(x)$  is the usual Hamming weight of  $\mathbf{r}_n(x)$ ,
- (3)  $\text{Step}_n(x)$  is the unique  $i$  such that  $\text{SBC}(n, i) \leq x2^n < \text{SBC}(n, i + 1)$ ,
- (4)  $S_n^*(x) = -n + 2\text{Step}_n(x)$ .
- (5)  $\text{Step}_n(x)$ ,  $\text{Weight}_n(x)$  depend at most on  $\mathbf{r}_n(x)$ . □

In view of (1.3) and 5. of Remark 1, we have defined  $\text{IStep}_n(k)$ ,  $\text{IWeight}_n(k)$ . We already knew that  $S_n$  and  $S_n^*$  also depend at most on  $\mathbf{r}_n(x)$  and thus we have also defined  $\text{IS}_n^*(k)$ ,  $\text{IS}_n(k)$  for  $k < 2^n$ ; by the usual identification, we have also defined  $\text{IS}_n^*(\mathbf{r})$ ,  $\text{IS}_n(\mathbf{r})$  for  $\mathbf{r} \in \{0, 1\}^n$ . Also,  $\text{IWeight}_n(k)$  is the usual Hamming weight of the binary representation of  $k$  and is therefore independent of  $n$ , so henceforth this will simply be denoted by  $\text{Weight}(k)$ . Similarly  $\text{Weight}(\mathbf{r})$  denotes the usual Hamming weight of  $\mathbf{r}$  for finite bitstrings,  $\mathbf{r}$ . *In what follows, we shall use the notation  $\text{IStep}(n, k)$  rather than  $\text{IStep}_n(k)$ .* The following is then also obvious

*Remark 2.* For  $n > 0$  and  $k < 2^n$ :

- (1)  $\text{IStep}(n, 0) = 0$  and for  $0 < k < 2^n$ ,  $\text{IStep}(n, k)$  is the least positive  $i \leq n$  such that  $k < \text{SBC}(n, i + 1)$ ,
- (2) For all  $i \in \mathbb{N}$ ,  $2^i - 1$  is the least  $k$  such that  $\text{Weight}(k) = i$  and  $2^n - 2^{n-i}$  is the largest  $k < 2^n$  such that  $\text{Weight}(k) = i$ ,
- (3) For all  $0 \leq i \leq n$ ,  $\text{SBC}(n, i)$  is the least  $k$  such that  $\text{IStep}(n, k) = i$ . □

**Definition 2.** For  $i \leq n$ , we define  $A_{n,i}$ ,  $B_{n,i}$  by:

$$A_{n,i} := \{x \in (0, 1) | \text{Step}_n(x) = i\},$$

$$B_{n,i} := \{x \in (0,1) \mid \text{Weight}_n(x) = i\}.$$

In view of Remark 2, for fixed  $n > 0$ , each of the  $A_{n,i}$ ,  $B_{n,i}$  is the union of level  $n$  dyadic intervals, and therefore, in view of the last paragraph of (1.3),  $IA_{n,i}$ ,  $IB_{n,i}$  will be used to denote the corresponding subsets of  $\{0, \dots, 2^n - 1\}$  (or of  $\{0, 1\}^n$ , via the usual identification) :

$$(4) \quad IA_{n,i} := \{k < 2^n \mid D_{n,k} \subseteq A_{n,i}\} \text{ and } IB_{n,i} := \{k < 2^n \mid D_{n,k} \subseteq B_{n,i}\}.$$

We also let  $\alpha_{n,i} := |IA_{n,i}|$ ,  $\beta_{n,i} := |IB_{n,i}|$  and for positive integers,  $x < 2^n$ , we let  $\alpha(n, i, x) = |IA_{n,i} \cap \{1, \dots, x\}|$ ,  $\beta(n, i, x) = |IB_{n,i} \cap \{1, \dots, x\}|$ .

This provides the motivating paradigm for the next definition, taking  $d = 1$ ,  $U_n = \{0, \dots, n\}$  and  $X_{n,i} = IA_{n,i}$  or  $X_{n,i} = IB_{n,i}$ .

**Definition 3.** Suppose that  $d \in \mathbb{Z}^+$  and that for  $n > 0$ ,  $U_n \subseteq \{0, \dots, n\}^d$ . Suppose, further, that for  $u \in U_n$ , we have non-empty  $X_{n,u} \subseteq \{0, \dots, 2^n - 1\}$ , with the increasing enumeration of  $X_{n,u}$  denoted by  $(x_{n,u,s} \mid 1 \leq s \leq |X_{n,u}|)$ . We define  $RX(n, u, \ell)$  to be that  $d + 2$  - place relation on  $\mathbb{N}$  such that

$$RX(n, u, \ell) \text{ iff } \ell \in X_{n,u}.$$

The *cardinality function associated with*  $RX$  is the function  $\text{cd}_{RX}$  which, for  $n > 0$ ,  $u \in U_n$  and positive integers,  $x < 2^n$ , assigns to  $(n, u, x)$ ,  $\text{cd}_{RX}(n, u, x) := |X_{n,u} \cap \{1, \dots, x\}|$ . We denote by  $ERX$  the enumerating function for  $RX$ :  $ERX(n, u, s) := x_{n,u,s}$  for  $1 \leq s \leq |X_{n,u}|$ . We will call  $RX$  *tame* if  $\text{cd}_{RX}$  is P-TIME.

In our invocations of Definition 3, we will have  $d = 1$  and  $U_n = \{0, \dots, n\}$  (for the first two invocations, and the last one) or  $d = 2$  and  $U_n = \{(i, j) \mid i, j \leq n, i \neq j\}$  (for the third and fourth invocations). In all of our invocations, it will be true that for fixed  $n$ ,  $\{X_{n,u} \mid u \in U_n\}$  will be a pairwise disjoint family, but we have not built this into the definition of tame.

**We now invoke Definition 3 with  $d = 1$  and  $U_n = \{0, \dots, n\}$  and with  $X_{n,i} = IA_{n,i}$  or  $X_{n,i} = IB_{n,i}$ .** This defines  $RIA$ ,  $RIB$ ,  $\text{cd}_{RIA}$ ,  $\text{cd}_{RIB}$ ,  $ERIA$ ,  $ERIB$ . The notation for the increasing enumerations will be  $a_{n,i,s}$ ,  $b_{n,i,s}$ .

*Remark 3.* The following observations are immediate, with the exception of item 6.

- (1) For fixed  $n, i, j$  we'll have that  $RIA(n, i, \ell)$  holds  $n > 0, 0 \leq i \leq n, 0 \leq \ell < 2^n$  and  $IStep(n, \ell) = i$ . Similarly,  $RIB(n, j, \ell)$  holds iff  $n > 0, 0 \leq j \leq n, 0 \leq \ell < 2^n$  and  $\text{Weight}(\ell) = j$ .
- (2)  $\text{cd}_{RIA}$  is the function  $\alpha$  of Definition 2 while  $\text{cd}_{RIB}$  is the function  $\beta$  of Definition 2. If  $x < \text{SBC}(n, i)$ , then  $\alpha(n, i, x) = 0$ , and if  $x \geq \text{SBC}(n, i + 1)$ , then  $\alpha(n, i, x) = \binom{n}{i} = \text{SBC}(n, i + 1) - \text{SBC}(n, i)$ . For  $\text{SBC}(n, i) \leq x < \text{SBC}(n, i + 1)$ ,  $\alpha(n, i, x) = x + 1 - \text{SBC}(n, i)$ .
- (3) For  $n > 0$ ,  $\alpha_{n,i} = |IA_{n,i}| = \binom{n}{i} = |IB_{n,i}| = \beta_{n,i}$ .
- (4) If  $a = a_{n,i,s}$ , then  $s = \alpha(n, i, a)$  and  $a = \text{ERIA}(n, i, s)$ ; the analogous statements hold, replacing  $A$  with  $B$ ,  $\alpha$  with  $\beta$  and all occurrences of  $a$  with  $b$ .
- (5) For any system  $X_{n,u}$  as in Definition 3, if  $u \in U_n$ ,  $a < b < 2^n$ , then  $\text{cd}_{RX}(n, u, b) - \text{cd}_{RX}(n, u, a) = |\{x \in X_{n,u} \mid a < x \leq b\}|$ .
- (6) Suppose that  $\{(n, u) \mid u \in U_n\}$  is P-TIME decidable. Then, if  $RX$  is tame, it is also P-TIME decidable.

*Proof.* Items 1. - 5. are obvious. For item 6., note that for  $n > 0$ ,  $u \in U_n$  and  $x \in \mathbb{Z}^+$  with  $x < 2^n$ ,  $RX(n, u, x)$  holds iff either  $x = \text{cd}_{RX}(n, u, x) = 1$  or  $(x > 1 \text{ and } \text{cd}_{RX}(n, u, x) = \text{cd}_{RX}(n, u, x - 1) + 1)$ .  $\square$

**Lemma 1.** *Let  $n > 0$ . Then:*

- (1) *If  $\pi$  is a permutation of  $\{0, \dots, 2^n - 1\}$ , the admissibility of  $\pi$  is equivalent to each of the following conditions:*
  - (a) *for all  $k < 2^n$ ,  $\text{Weight}(\pi(k)) = IStep(n, k)$ ,*
  - (b) *for all  $i < n$ ,  $\pi[IA_{n,i}] = IB_{n,i}$ ,*
  - (c)  $IS_n^* = IS_n \circ \pi$ .

(2) There are  $\prod_{i=0}^n \binom{n}{i}!$  admissible permutations of  $\{0, \dots, 2^n - 1\}$ .

*Proof.* For 1., it is clear that (b) and (c) are each equivalent to (a), so we argue that the admissibility of  $\pi$  is equivalent to (a). Let  $\pi$  be any permutation of  $\{0, \dots, 2^n - 1\}$ , let  $k < 2^n$  and let  $x \in D_{n,k}$ ,  $y \in D_{n,\pi(k)}$ . Then:

$$2\text{ISStep}(n, k) = n + S_n^*(x) \text{ and } 2\text{Weight}(\pi(k)) = n + S_n(y).$$

But the condition that the right hand sides of the last two displayed equations are equal (for any  $k$  and any such  $x, y$ ) defines the admissibility of  $\pi$ , while (a) is the condition that the left hand sides are equal (for all  $k$ ), and so the admissibility of  $\pi$  is equivalent to (a).

For 2., note that an admissible permutation  $\pi$  decomposes into the system of its restrictions to the  $IA_{n,i}$ . Complete information about  $\pi \upharpoonright IA_{n,i}$  is encoded by the permutation,  $\bar{\pi}_{n,i}$  of  $\{1, \dots, \binom{n}{i}\}$  defined by:

$$(5) \quad \text{if } 1 \leq s \leq \binom{n}{i}, \text{ then } \bar{\pi}_{n,i}(s) := \beta(n, i, \pi(a_{n,i,s})).$$

Further, the  $\bar{\pi}_{n,i}$  are arbitrary in the sense that if, for  $i < n$ ,  $\sigma_{n,i}$  is any permutation of  $\{1, \dots, \binom{n}{i}\}$ , then for each  $n$  there is a (unique) admissible permutation  $\pi_n$  of  $\{0, \dots, 2^n - 1\}$  such that for each  $i < n$ ,  $\bar{\pi}_{n,i} = \sigma_{n,i}$ . Finally, for fixed  $n$ , the product in 2. counts the number of such systems ( $\sigma_{n,i} | i < n$ ), and so 2. follows.  $\square$

It is worth pointing out, here, that the proof of 2. of Lemma 1 provides us with yet another view of admissible permutations, since they correspond canonically to such systems of  $\sigma_{n,i}$ . We will return to this view of admissible permutations in (3.5) below.

**3.2. Corollary 2 and Propositions 1, 2.** The next Corollary is an immediate consequence of Theorem 1, Corollary 1 and 2. of Lemma 1; it gives the existence of trim, strong triangular array for  $\{S_n^*\}$ .

**Corollary 2.** For each  $n$ , there are  $\prod_{i=0}^n \binom{n}{i}!$  representations

$$S_n^* = \sum_{i=1}^n R_{n,i}^*,$$

where  $(R_{n,i}^* | 1 \leq i \leq n)$  is an independent family of Rademacher random variables each of which has mean 0, variance 1 and depends only on  $\mathbf{r}_n$ . Therefore, there exist (continuum many) trim, strong triangular array representations of the sequence  $\{S_n^*\}$ .  $\square$

The next Proposition builds on Corollary 2 to show that there are non-trim, strong triangular array representations of  $\{S_n^*\}$ , by constructing one, as a modification of a trim, strong one. Thus, the existence of trim strong triangular arrays for  $\{S_n^*\}$  is not an immediate formal consequence of the existence of strong ones.

**Proposition 1.** There are non-trim, strong triangular arrays for  $\{S_n^*\}$ .

*Proof.* Fix a trim, strong triangular array,  $\{R_{n,i}^*\}$ , for  $\{S_n^*\}$ . It is easy to see that for all sufficiently large  $n$  we can find  $i_1, i_2, k_1, k_2$  such that  $i_1 \neq i_2$ ,  $i_1, i_2 < n$ ,  $k_1 < k_2 < 2^n$  and for  $j = 1, 2$ :

$$R_{n,i_1}^*(x) = (-1)^j \text{ for all } x \in D_{n,k_j} \text{ and } R_{n,i_2}^*(x) = (-1)^{j-1} \text{ for all } x \in D_{n,k_j}.$$

Fixing a sufficiently large  $n^*$  and then fixing such  $i_1, i_2, j_1, j_2$ , we define  $\{R_{n,i}^{**}\}$  and then verify that it is a non-trim, strong triangular array for  $\{S_n^*\}$ . For  $n \neq n^*$ , or  $n = n^*$  and  $i \neq i_1, i_2$ , we let  $R_{n,i}^{**} := R_{n,i}^*$ . For  $j = 1, 2$ , we let:

$$R_{n^*,i_1}^{**}(x) := (-1)^j \text{ for all } x \in D_{n^*+1,2k_1+j-1} \cup D_{n^*+1,2k_2+2-j} \text{ and}$$

$$R_{n^*,i_1}^{**}(x) := (-1)^{j-1} \text{ for all } x \in D_{n^*+1,2k_1+2-j} \cup D_{n^*+1,2k_2+j-1},$$

$$R_{n^*,i_2}^{**}(x) := (-1)^j \text{ for all } x \in D_{n^*+1,2k_1+2-j} \cup D_{n^*+1,2k_2+j-1} \text{ and}$$

$$R_{n^*,i_2}^{**}(x) := (-1)^{j-1} \text{ for all } x \in D_{n^*+1,2k_1+j-1} \cup D_{n^*+1,2k_2+2-j}.$$

Clearly  $R_{n^*,i_1}^{**}$ ,  $R_{n^*,i_2}^{**}$  are Rademacher, with mean 0 and variance 1 and clearly they depend on  $\varepsilon_{n^*+1}$ . By construction, we have guaranteed that for all  $x \in D_{n^*,k_1} \cup D_{n^*,k_2}$  we will have that

$$\begin{aligned} R_{n^*,i_1}^{**}(x) + R_{n^*,i_2}^{**}(x) &= R_{n^*,i_1}^*(x) + R_{n^*,i_2}^*(x) \text{ and} \\ R_{n^*,i_1}^{**}(x) \cdot R_{n^*,i_2}^{**}(x) &= R_{n^*,i_1}^*(x) \cdot R_{n^*,i_2}^*(x). \end{aligned}$$

This suffices to show that the  $R_{n^*,i}^{**}$  are independent, and that they sum to  $S_{n^*}$ . Thus,  $\{R^{**}\}$  is a strong, non-trim triangular array for  $\{S_n^*\}$ , as required.  $\square$

The next Proposition is a “non-persistence” result, showing that in any sequence,  $\{\pi_n\}$ , of admissible permutations, there is no  $n$  such that  $\pi_{n+1}$  extends  $\pi_n$ , and that, in any trim, strong triangular array representation,  $\{R_{n,i}^*\}$ , of  $\{S_n^*\}$ , for any  $n$ , there is some  $i$  such that  $R_{n+1,i}^* \neq R_{n,i}^*$ . This is in contrast to the situation for the  $R_{n,i}$ , so, as noted at the end of (1.2.2), Proposition 2 begins to answer to Question 4. Item 1. of Proposition 2 appeals to 1. of Lemma 1.

**Proposition 2.**

- (1) If  $\{\pi_n\}$  is any sequence of admissible permutations, then for all  $n$ ,  $\pi_n \not\subseteq \pi_{n+1}$ .
- (2) If  $\{R_{n,i}^*\}$  is a trim, strong triangular array for  $\{S_n^*\}$ , then for all  $n$ , there is  $1 \leq i \leq n$  such that  $R_{n+1,i}^* \neq R_{n,i}^*$ .

*Proof.* For item 1., the most obvious obstacle to having  $\pi_n \subseteq \pi_{n+1}$  is that there will be  $k < 2^n$  such that  $\text{IStep}(n+1, k) < \text{IStep}(n, k)$ . Since  $\text{Weight}(\pi_i(k)) = \text{IStep}(i, k)$ , for  $i = n, n+1$ , clearly  $\text{Weight}(\pi_{n+1}(k)) < \text{Weight}(\pi_n(k))$ , and therefore  $\pi_{n+1}(k) \neq \pi_n(k)$ , for any such  $k$ .

For item 2., note first that

$$\text{for any } k < 2^n, D_{n,k} = D_{n+1,2k} \cup D_{n+1,2k+1}.$$

Now, let  $\{R_{n,i}^*\}$  be a trim, strong triangular array for  $\{S_n^*\}$ , and  $\{\pi_n\}$  be the associated sequence of admissible permutations. Fix  $n$ , and, towards a contradiction, assume that  $R_{n+1,i}^* = R_{n,i}^*$  for all  $1 \leq i \leq n$ . We first show that

$$\text{for all } k < 2^n \text{ and for } j = \pi_{n+1}(2k), \pi_{n+1}(2k+1), D_{n+1,j} \subseteq D_{n,\pi_n(k)}.$$

We argue this for  $j = \pi_{n+1}(2k)$ . The case  $j = \pi_{n+1}(2k+1)$  is similar. Note that

$$\text{for all } 1 \leq i \leq n, y \in D_{n+1,j} \text{ and } x \in D_{n+1,2k}, (-1)^{1+\varepsilon_i(y)} = R_{n+1,i}^*(x).$$

But any such  $x$  is in  $D_{n,k}$ , and, by hypothesis,  $R_{n+1,i}^*(x) = R_{n,i}^*(x)$ , so

$$(-1)^{1+\varepsilon_i(y)} = R_{n+1,i}^*(x) = R_{n,i}^*(x) = (-1)^{1+\varepsilon_i(z)} \text{ for any } z \in D_{n,\pi_n(k)},$$

i.e.,  $y \in D_{n,\pi_n(k)}$ . It is then immediate that

$$\begin{aligned} D_{n,\pi_n(k)} &= D_{n+1,\pi_{n+1}(2k)} \cup D_{n+1,\pi_{n+1}(2k+1)} \text{ and so:} \\ \{\pi_{n+1}(2k), \pi_{n+1}(2k+1)\} &= \{2\pi_n(k), 2\pi_n(k)+1\}, \end{aligned}$$

which means that  $\pi_{n+1}(2k), \pi_{n+1}(2k+1)$  have opposite parity. Now, however, choose  $k > 0$  so that  $\text{IStep}(n+1, 2k) = \text{IStep}(n+1, 2k+1) = 1$  and  $\pi_{n+1}(2k), \pi_{n+1}(2k+1) > 1$ . Then  $\pi_{n+1}(2k), \pi_{n+1}(2k+1)$  both have weight 1 and therefore, both are even, contradiction!  $\square$

**3.3. Sequences of Admissible Permutations and their Encodings, Proposition 3.** A sequence,  $\{\pi_n\}$  of permutations of  $\{0, \dots, 2^n - 1\}$  (admissible or not) is naturally encoded by the two-place function  $\Pi : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$  defined by  $\Pi(n, k) = \pi_n(k)$  for  $n > 0$  and  $k < 2^n$ ,  $\Pi(0, 0) = 0$  and  $\Pi(n, k) = 2^n$ , for  $k \geq 2^n$  (including when  $n = 0$  and  $k > 0$ ). We will approach the question of the complexity of the sequence in terms of the complexity of its natural encoding.

The next Proposition gives our general lower complexity bound statement for arbitrary sequences of admissible permutations. We follow the general approach developed in the first paragraph of (1.3.5).

**Proposition 3.** *The complexity of  $2^n$  is a lower bound for the complexity of any sequence of admissible permutations, and thus for any trim, strong triangular array for  $\{S_n^*\}$ .*

*Proof.* Let  $\{\pi_n\}$  be any sequence of admissible permutations and let  $\Pi$  be its natural encoding. A simple, explicit expression for  $2^n$  in terms of the  $n$  values,  $\Pi(n, 1), \dots, \Pi(n, n)$ , of  $\Pi$ , uniformly in  $n$  is provided by Equation (6), below. Thus, by paragraph 1 of (1.3.5) Equation (6) and its proof give the statement of the proposition.

$$(6) \quad \text{For all } n > 0, \quad 2^n = 1 + \sum_{i=1}^n \Pi(n, i).$$

Equation 6 is immediate, from the following observations. First,  $IA_{n,1} = \{1, \dots, n\}$ . Second,  $IB_{n,1}$  is the set of powers of 2 below  $2^n$  (since these are the weight 1 positive integers below  $2^n$ ). Finally,  $\pi_n [IA_{n,1}] = IB_{n,1}$ .  $\square$

**3.4. The sequence  $\{F_n\}$ , its natural encoding,  $F$ , and Theorem 2.** For the next Definition, recall our invocation of Definition 3 in (3.1, where the  $b_{n,i,s}$  and  $\alpha(n, i, k)$  are defined).

**Definition 4.** For all  $n > 0$ ,  $F_n$  is the permutation of  $\{0, \dots, 2^n - 1\}$  defined as follows. If  $0 \leq k < 2^n$ , let  $i = \text{IStep}(n, k)$ . Then

$$F_n(k) := b_{n,i,s}, \text{ where } s = \alpha(n, i, k).$$

Then, take  $F : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$  to be the natural encoding of the sequence  $\{F_n\}$ . Also, for use in (3.5) and referring to the first sentence of (3.3), we take  $\text{Inv}F : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$  to be the natural encoding of the sequence  $\{F_n^{-1}\}$ .

In view of 2. of Lemma 1, these  $F_n$  are (obviously) very natural admissible permutations of the  $\{0, \dots, 2^n - 1\}$ . Recalling that, ERIB is the enumerating function for RIB, viz. the invocation of Definition 3 immediately preceding Remark 3, note that  $F(n, k) = \text{ERIB}(n, i, s)$ , where  $s$  is as in Definition 4.

*Remark 4.* Note that our definition of  $F_n$  is equivalent to stipulating that, in terms of the notation used in Equation (5), for all  $i \leq n$ ,  $\overline{F}_n$  is the identity permutation of  $\{1, \dots, \binom{n}{i}\}$ . Note, also, that with  $i = \text{IStep}(n, k)$  and  $s = \alpha(n, i, k)$ , then, in fact,  $s = k - \text{SBC}(n, i)$ ; further, for these  $i, s$ , we also have that  $s = \beta(n, i, F(n, k))$ .  $\square$

**Proposition 4.** *As functions of  $(n, i)$ , with  $i \leq n$ , the binomial coefficients  $\binom{n}{i}$  and SBC are computable in time polynomial in  $n$ . The function IStep is P-TIME. Further, the relation RIA is tame.*

*Proof.* The algorithm for computing the binomial coefficients is simply to generate the needed portion of Pascal's triangle using the familiar addition identity. This requires  $O(n^2)$  additions, and then the computation of  $\text{SBC}(n, i)$ , requires  $i$  more additions. All of the summands remain below  $2^n$ , obviously. For additional results on the computation of the binomial coefficients, see [1], [6]. That IStep is P-TIME then follows immediately from item 1. of Remark 2; note that the "search" is bounded by  $n$ . For the final statement, recall (item 2. of Remark 3) that the function  $\alpha$  of Definition is  $\text{cd}_{\text{RIA}}$ , and let  $x \in \mathbb{Z}^+$ . Note that if  $x < \text{SBC}(n, i)$ , then  $\alpha(n, i, x) = 0$ , and if  $x \geq \text{SBC}(n, i + 1) - 1$ , then  $\alpha(n, i, x) = \binom{n}{i}$ . For  $\text{SBC}(n, i) \leq x < \text{SBC}(n, i + 1) - 1$ ,  $\alpha(n, i, x) = 1 + x - \text{SBC}(n, i)$ , by Remark 4. Thus,  $\alpha$  is P-TIME.  $\square$

The next Lemma embodies, in abstract form (to facilitate multiple applications), S. Buss's suggestion of combining tameness with a binary search argument to show that if  $\text{RX}$  is tame then  $\text{ERX}$  is P-TIME. Along with Item 6. of Remark 3, Lemma 2 represents the main apport of the hypothesis of tameness.

**Lemma 2.** *Suppose that  $U_n$ , the  $X_{n,u}$ , etc., are as in Definition 3 and suppose that  $\text{RX}$  is tame. Then the enumerating function  $\text{ERX}$  is P-TIME.*

*Proof.* Fix  $n, u \in U_n$  and  $s$  with  $1 \leq s \leq |X_{n,u}|$ . Let  $\text{cd} = \text{cd}_{\text{RX}}$  be the cardinality function associated with the  $X_{n,u}$ ; by hypothesis,  $\text{cd}$  is P-TIME. Start from  $a_0 = 0, b_0 = 2^n - 1, s_0 = s$ . Having defined  $a_i, b_i, s_i$ , we let  $m_i := \lfloor (a_i + b_i) / 2 \rfloor$  and we consider whether  $\text{cd}(n, u, m_i) - \text{cd}(n, u, a_i) \geq s_i$ . If so, we take  $a_{i+1} = a_i, b_{i+1} = m_i, s_{i+1} = s_i$ . Otherwise, we take  $a_{i+1} =$

$m_i, b_{i+1} = b_i, s_{i+1} = s_i + \text{cd}_{RX}(n, u, a_i) - \text{cd}_{RX}(n, u, m_i)$ . Then, clearly, for some  $k \leq n$  we will have  $s_k = 1, a_k = b_k - 1$  and  $b_k = x_{n,u,s}$ . Thus,  $ERX$  is P-TIME.  $\square$

S. Buss also sketched for us an argument that became the proof of the next Lemma.

**Lemma 3.** (S. Buss) *RIB is tame.*

*Proof.* We show that the function  $\beta$  of Definition 2 is P-TIME. This suffices, since by (2) of Remark 3,  $\beta$  is  $\text{cd}_{RIB}$ . Let  $j \leq n$  and let  $b \in \mathbb{N}$  with  $b < 2^n$ . Without loss of generality we may assume  $0 < j, b$  and  $j < n$ . Let  $\ell = \min(j, \text{Weight}(b))$ , so  $\ell \geq 1$ . Let  $i_1 > \dots > i_\ell$  be the  $\ell$  largest  $i$ 's such that the  $i^{\text{th}}$  bit in the binary expansion of  $b$  is 1. Clearly  $\ell$  and the  $i_s$  are computed in time polynomial in  $n$ .

If  $j > i_1$ , then  $\beta(n, j, b) = 0$ , so assume that  $j \leq i_1$ . If  $j = 1$ , then clearly  $\beta(n, 1, b) = i_1$ , so assume that  $j > 1$  and so  $i_1 > 1$ . If  $x \in \mathbb{N}$  with  $x \leq b$ , then either  $x = b$  or there is unique  $s$  with  $1 \leq s \leq \ell$  such that the  $s$ -th bit in the binary expansion of  $x$  is 0 but for all  $1 \leq t < s$ , the  $t$ -th bit in the binary expansion of  $x$  is 1.

Note that if  $1 \leq s \leq \ell$ , then  $\binom{i_s-1}{j+1-s}$  counts the number of such  $x < b$  with  $\text{Weight}(x) = j$ . Finally, this means that if  $\text{Weight}(b) = j$ , then  $\beta(n, j, b) = 1 + \sum_{s=1}^{\ell} \binom{i_s-1}{j+1-s}$ , while otherwise,  $\beta(n, j, b) = \sum_{s=1}^{\ell} \binom{i_s-1}{j+1-s}$ .  $\square$

We record a few observations related to the proof of Lemma 3 that will be useful in the proof of Theorem 2. First, note that, for  $i_s = 1$ , the binomial coefficient  $\binom{i_s-1}{j+1-s}$  is just 1; for  $i_s > 1$ , the coefficients that occur in the final paragraph of the proof can be expressed in terms of SBC:

$$\binom{i_s-1}{j+1-s} = \text{SBC}(i_s-1, j+2-s) - \text{SBC}(i_s-1, j+1-s).$$

Thus, the function  $\beta$  has a simple expression in terms of SBC. Next, note that  $\chi_{RIB}(n, j, x) = 1$  iff ( $j = x = 1$  or ( $x > 1$  and  $\beta(n, j, x) = \beta(n, j, x-1) + 1$ )). Thus,  $\chi_{RIB}$  also has a simple expression in terms of SBC, since  $\beta$  does. This is similar to the argument for item 6. of Remark 3.

Since  $\text{Weight}$  does not depend on  $n$ , we can naturally “put together” the different branches, indexed by  $n$ , of the  $ERIB$  function into a single enumerating function,  $EW$ , for  $\text{Weight}$ ; this is Definition 5. The final assertion of Corollary 3 is an easy consequence of Lemmas 2, 3:  $EW$  is P-TIME. This result is used in the proof of Theorem 2 and is also of some interest in its own right, since the sequence <http://oeis.org>, 2010, Sequence A066884, [9], encodes  $EW$ ; [9] does not indicate that this sequence is P-TIME and gives no closed form.

**Definition 5.** For  $j, t \in \mathbb{N}$ :

$$EW(j, t) := \begin{cases} 0, & \text{if } j = 0 \\ \text{the } t^{\text{th}} m \text{ such that } \text{Weight}(m) = j & \text{if } j > 0 \end{cases}$$

**Corollary 3.** *The relations RIA, RIB are P-TIME decidable. The function EW is P-TIME. The relation between  $n, k, m$  expressed by the Equation 7, which follows, is also P-TIME decidable. Given  $n$  and  $k < 2^n$ , this equation has a unique solution,  $m$ , which, as a function of  $(n, k)$ , is also P-TIME.*

$$(7) \quad \beta(n, \text{IStep}(n, k), m) \cdot \chi_{RIB}(n, \text{IStep}(n, k), m) = \alpha(n, \text{IStep}(n, k), k).$$

*Proof.* By Proposition 4, RIA is tame, and by Lemma 3, so is RIB. Since the hypothesis of item 6. of Remark 3 clearly holds for RIA, RIB, these relations are P-TIME decidable.

For  $EW$ , note that if  $j > 0$ , then for any  $t$ , taking  $n = \max(j, t) + 1$ , we will have  $t \leq \binom{n}{j}$ . Therefore,  $EW(j, t) < 2^n$ , and so  $EW(j, t) = ERIB(n, j, t)$ . Since RIB is P-TIME decidable,  $\chi_{RIB}$  is P-TIME, and so the third sentence of the Corollary is immediate from Lemma 3 and the first sentence.

Let  $j = \text{IStep}(n, k)$  and note that  $\alpha(n, j, k) > 0$ . This is the point of multiplying by  $\chi_{\text{RIB}}(n, j, m)$ : to ensure that  $m \in \text{IB}_{n, j}$ . The unique solution  $m$  is computed as  $\text{EW}(j, k + 1 - \text{SBC}(n, j))$ .  $\square$

The observations in the last paragraph of the proof of Corollary 3 will be used in the proof of Theorem 2. Of course the P-TIME decidability of RIA can be established quite simply and directly from Proposition 4, but the approach taken is more efficient.

**Theorem 2.**  $F$  is P-TIME and simply computed in terms of SBC.

*Proof.* We first argue for the lower complexity bound much as in Proposition 3, but with a slightly cleaner expression for  $2^n$  given by Equation (8), below, rather than by Equation (6). We then show that  $F$  is P-TIME; the upper complexity bound then follows by the general argument given in (1.3.5). We note:

$$(8) \quad 2^n = F(n, n) + F(n, n).$$

For Equation (8), the relevant observations are that  $n$  is the largest element of  $\text{IA}_{n, 1}$ ,  $2^{n-1}$  is the largest element of  $\text{IB}_{n, 1}$  and that for all  $n, i$ ,  $F_n$  maps  $\text{IA}_{n, i}$  onto  $\text{IB}_{n, i}$  in order-preserving fashion.

The rest of the proof follows the strategy laid out in (1.3.5). To see that  $F$  is P-TIME we will argue that

$$(9) \quad \text{For } n > 0 \text{ and } k < 2^n, m = F(n, k) < 2^n \text{ is the unique solution of Equation (7).}$$

This is immediate from the last observation given in connection with Equation (8) and clearly suffices to show that  $F$  is P-TIME, in view of Lemmas 2, 3 and Corollary 3. That  $F$  is simply computed in terms of SBC follows from Equation (7) since all of the functions that figure there are simply computed in terms of SBC. For  $\text{IStep}$ , this is by item 1. of Remark 2. For  $\alpha$ , this is by item 2. of Remark 3. For  $\beta$  and  $\chi_{\text{RIB}}$  this is by the first paragraph following the proof of Corollary 3.  $\square$

**3.5. Obtaining SBC and related Questions.** We begin by showing how to obtain SBC from  $F$  and  $\text{Inv}F$  (the latter was also introduced in Definition 4).

**Corollary 4.** SBC is simply computed in terms of  $F$  and  $\text{Inv}F$ .  $\text{Inv}F$  is simply computed in terms of SBC. Thus, the joint complexity of  $F$  and  $\text{Inv}F$  is exactly that of SBC.

*Proof.* For the first assertion, recall that  $\text{SBC}(n, 0) = 0$  and note that  $\text{SBC}(n, n + 1) = 2^n$ . For  $1 \leq i \leq n$ , note that  $\text{SBC}(n, i) = \text{Inv}F(n, 2^i - 1)$ . But  $2^i - 1 = 2F(i, i) - 1$ .

That  $\text{Inv}F$  is simply computable from SBC follows from the material of (3.4), and in particular from the following ‘‘dual version’’ (interchanging Step and Weight) of Equation 7:

$$\alpha(n, \text{Weight}(m), k) \cdot \chi_{\text{RIA}}(n, \text{Weight}(n, m), k) = \beta(n, \text{Weight}(m), m).$$

As in (3.4), all of the functions in the previous displayed equation are simply computed from SBC, and, given  $(n, m)$ , the unique solution,  $k$ , is computed as  $\text{SBC}(n, \text{Weight}(m), t)$ , where  $m = \text{EW}(\text{Weight}(m), t)$ . We can easily compute  $t$  from SBC (and EW) using a binary search argument with initial interval  $\left[1, \binom{n}{\text{Weight}(m)}\right]$ . But this unique solution is just  $\text{Inv}F(n, m)$ . The final assertion is immediate from the first two.  $\square$

*Remark 5.* It would be ideal if we could show that SBC is simply computed from  $F$  alone, since then the complexity of  $F$  would be exactly that of SBC. The specific obstacle is being able to carry out the calculation of  $t$  in the last sentence of the proof of the Corollary in terms of  $F$  alone, without the use of the binomial coefficient or the function EW. An indication that this obstacle may be serious is the general phenomenon that an inverse of a function,  $f$ , can be significantly more complex than  $f$  itself. Symmetrically, if we could eliminate the use of  $F$  to compute  $2^i - 1$ , it would follow that the complexity of  $\text{Inv}F$  is exactly that of SBC. This seems somewhat more feasible.

We conclude this section by tying up some “odds and ends”. We first argue that  $\{F_n\}$  is the simplest sequence of admissible permutations, and so its corresponding triangular array representation is the simplest trim, strong triangular array representation for  $\{S_n^*\}$ . Finally, we make some observations concerning the contrast between Equations (6) and (8) in light of this status of  $\{F_n\}$ .

Remark 4 and the proof of item 2. of Lemma 1 are the main elements of our argument that  $\{F_n\}$  is the simplest sequence of admissible permutations. Recall that each  $F_n \upharpoonright IA_{n,i}$  is the order-preserving bijection between  $IA_{n,i}$  and  $IB_{n,i}$ . While the claim that this is the simplest bijection between these sets may not be entirely clear, it is far clearer that the identity permutation on  $\{1, \dots, \binom{n}{i}\}$  is the simplest permutation of this set. By Remark 4, each  $\bar{F}_{n,i}$  is the identity permutation on  $\{1, \dots, \binom{n}{i}\}$  and so from the point of view of the proof of Lemma 1 and the subsequent paragraph,  $\{F_n\}$  really is simplest, since it is represented by the system where each  $\sigma_{n,i}$  is the identity permutation. It should, however, be acknowledged that we have “built in” the role of the increasing enumerations in this way of representing admissible permutations.

Regarding the contrast between Equations (6) and (8), what is really at issue is to be able to easily identify  $k(n) = (\pi_{n+1})^{-1}(2^n)$  as a function of  $n$ , since, trivially, we’ll always have that  $2^n = \pi_{n+1}(k(n))$ . For  $\{F_n\}$ , Equation (8) is based on the easy identification of  $k(n)$  as simply being  $n + 1$ . It is then natural to expect that for more complex sequences  $\{\pi_n\}$ , the corresponding function  $k(n)$  will also be more complex, leaving us only Equation (6) rather than a simple analogue of Equation (8). This has some features in common with the issues discussed in Remark 5, above.

#### 4. CONSTRUCTION OF THE VARIANTS OF $F$ AND THEOREM 3

**4.1. The functions  $G$  and  $H$ .** Here we construct the variants,  $G$  (Definition 7) and  $H$  (Definition 11), of  $F$ . We impose additional requirements on the admissible permutations,  $G_n$  and  $H_n$ , respectively, that are to be encoded.

The motivation for introducing these variants is to obtain sequences of permutations whose natural encodings are still P-TIME, with SBC as an upper complexity bound (this will be the content of Theorem 3) and where the orbit structures of the individual permutations are simpler than those of the  $F_n$ . We construct the  $G_n$  so as to maximize the number of fixed points. The construction of the  $H_n$  goes farther: once all possible fixed points have been identified (the same ones as for the  $G_n$ ), we maximize the number of two-cycles, so that the  $H_n$  are as close as possible to being self-inverse.

We construct the  $G_n$  in two stages: we first note the fixed points are the elements of the  $IA_{n,i} \cap IB_{n,i}$ . We then proceed much as for  $F$ : for each  $1 \leq i \leq n$ , map “what is left of”  $IA_{n,i}$  in order preserving fashion onto “what is left of”  $IB_{n,i}$ . Of course, this requires that these two sets have the same cardinality; this will be obvious for the construction of  $G_n$ , as noted in Remark 6.

We construct the  $H_n$  in three stages, with the first stage being identical to the first stage in the construction of the  $G_n$ . We interpolate a new second stage, where we identify a maximal set of two-cycles. The third and final stage is analogous to the second stage in the definition of the  $G_n$ , in that, for each  $1 \leq i \leq n$ , we map “what is left of”  $IA_{n,i}$  in order preserving fashion onto “what is left of”  $IB_{n,i}$ . This time, “what is left” means after removing the fixed points *and* the points involved in the two-cycles identified in the second stage. As in the second stage of the construction of  $G_n$ , in order to carry out the third and final stage for the  $H_n$ , it must again be true that for each  $i$ , “what is left of”  $IA_{n,i}$  has the same cardinality as “what is left of”  $IB_{n,i}$ . This is the content of Proposition 5.

The constructions of the  $G_n$  and of the  $H_n$  will both be uniform in  $n$ , so for the remainder of this subsection, we take  $n$  to be fixed. The next definition is analogous to Definition 2. It introduces the  $IA_{n,i}^1$  and  $IB_{n,i}^1$ : “what is left of  $IA_{n,i}$ , resp.  $IB_{n,i}$ ”, after removing the fixed points.

**Definition 6.** For  $i < n$ ,  $IA_{n,i}^1 := IA_{n,i} \setminus (IA_{n,i} \cap IB_{n,i})$ ,  $IB_{n,i}^1 := IB_{n,i} \setminus (IA_{n,i} \cap IB_{n,i})$ . We also let  $\bar{\alpha}_{n,i}^0 = \bar{\beta}_{n,i}^0 := |IA_{n,i} \cap IB_{n,i}|$ , and set  $\alpha_{n,i}^1 := |IA_{n,i}^1|$ ,  $\beta_{n,i}^1 := |IB_{n,i}^1|$ .



We now invoke Definition 3 with  $d = 1$  and  $U_n = \{0, \dots, n\}$  and with  $X_{n,i} = IA_{n,i}^1$  or  $X_{n,i} = IB_{n,i}^1$ . This defines  $RIA^1$ ,  $RIB^1$ ,  $cd_{RIA^1}$ ,  $cd_{RIB^1}$ ,  $ERIA^1$ ,  $ERIB^1$ . We use  $\alpha^1$ ,  $\beta^1$  to denote  $cd_{RIA^1}$ ,  $cd_{RIB^1}$ , respectively. The notation for the increasing enumerations will be  $a_{n,i,s}^1$ ,  $b_{n,i,s}^1$ .

Remark 6. For  $i < n$ , the following observations are obvious:

- (1)  $\alpha_{n,i}^1 = \binom{n}{i} - \bar{\alpha}_{n,i}^0 = \binom{n}{i} - \bar{\beta}_{n,i}^0 = \beta_{n,i}^1$ ,
- (2) for  $k \in IA_{n,i}$ ,  $k \in IA_{n,i}^1$  iff  $\text{Weight}(k) \neq i$ ; for  $m \in IB_{n,i}$ ,  $m \in IB_{n,i}^1$  iff  $\text{IStep}(n, k) \neq i$ .  $\square$

**Definition 7.**  $G_n$  is the permutation of  $\{0, \dots, 2^n - 1\}$  defined as follows. If  $0 \leq k < 2^n$ , let  $i = \text{IStep}(n, k)$ , then:

$$(10) \quad G_n(k) := \begin{cases} k & \text{if } \text{Weight}(k) = i \\ b_{n,i,s}^1 & \text{where } s = \alpha^1(n, i, k), \text{ otherwise.} \end{cases}$$

Take  $G : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$  to be the natural encoding of the sequence  $\{G_n\}$ .

It is clear that  $G_n$  is an admissible permutation of  $\{0, \dots, 2^n - 1\}$ , with the additional property that  $G_n$  is the identity on  $k$  such that  $\text{IStep}(n, k) = \text{Weight}(k)$ , i.e.,  $G$  is maximal, among admissible permutations of  $\{0, \dots, 2^n - 1\}$ , for agreement with the identity permutation. Further, in analogy with Remark 4 and (3.5), we argue that  $G$  is the simplest such admissible permutation. This is based on the analogues of the  $\bar{F}_{n,i}$  defined on  $\{1, \dots, \alpha_{n,i}^1\}$ , starting from  $G_n \upharpoonright A_{n,i}^1$ . Each of these is the identity on  $\{1, \dots, \alpha_{n,i}^1\}$ .

We turn now to the definition of the  $H_n$  and  $H$ . Once again, we will proceed in analogy with Definitions 2 - 4. Our first task is to identify those  $k$  which will be part of a two-cycle.

In order to motivate what follows, suppose that  $\pi$  is an admissible permutation of  $\{0, \dots, 2^n - 1\}$  with the property we have built into  $G_n$ : that  $\pi(s) = s$  whenever  $\text{IStep}(n, s) = \text{Weight}(s)$ . Suppose further that  $k \neq m$ ,  $\pi(k) = m$  and  $\pi(m) = k$ . Let  $i = \text{IStep}(n, k)$ ,  $j = \text{Weight}(k)$ . Then  $i \neq j$ ,  $i = \text{Weight}(m)$ ,  $j = \text{IStep}(n, m)$ . Stated otherwise, we have that  $k \in IA_{n,i}^1 \cap IB_{n,j}^1$  and  $m \in IA_{n,j}^1 \cap IB_{n,i}^1$ .

**Definition 8.** For  $i, j < n$  with  $i \neq j$  we set:  $IC_{n,i,j}^1 := IA_{n,i}^1 \cap IB_{n,j}^1$ , and  $\gamma_{n,i,j}^1 := |IC_{n,i,j}^1|$ .

We now invoke Definition 3 with  $d = 2$  and  $U_n = \{(i, j) | 0 \leq i, j \leq n, i \neq j\}$  and with  $X_{n,i,j} = IC_{n,i,j}^1$ . This defines  $RIC^1$ ,  $cd_{RIC^1}$ ,  $ERIC^1$ . We use  $\gamma^1$  to denote  $cd_{RIC^1}$ . The notation for the increasing enumerations will be  $c_{n,i,j,s}^1$ .

Remark 7. The following observations are obvious:

$$\text{For } i < n, IA_{n,i}^1 = \bigsqcup_{0 \leq j < n, j \neq i} IC_{n,i,j}^1, \text{ and } IB_{n,i}^1 = \bigsqcup_{0 \leq j < n, j \neq i} IC_{n,j,i}^1. \quad \square$$

It would be natural to attempt to match up the elements of the  $IC_{n,i,j}^1$  with those of corresponding  $IC_{n,j,i}^1$  to form the two-cycles. However, the following example shows that even for fairly small  $n$ , this will not be possible, since it can happen that for certain  $i \neq j$ ,  $i, j < n$ ,  $\gamma_{n,i,j}^1 \neq \gamma_{n,j,i}^1$ . When  $n = 8$ , we have:

$$IC_{8,2,4}^1 = \{15, 23, 27, 29, 30\}, \text{ while } IC_{8,4,2}^1 = \{96, 129, 130, 132, 136, 144, 160\}.$$

When  $\gamma_{n,i,j}^1 > \gamma_{n,j,i}^1$  there are various reasonable ways of choosing the  $\gamma_{n,j,i}^1$  - many elements of  $IC_{n,i,j}^1$  which will form 2-cycles with the elements of  $IC_{n,j,i}^1$ . The particular way we have chosen in what follows is to *exclude* the "extreme" elements of  $IC_{n,i,j}^1$ : those that are farthest from the elements of  $IC_{n,j,i}^1$ . This is codified in the next Definition.

**Definition 9.** For  $i, j < n$  with  $i \neq j$ , let  $\bar{\gamma}_{n,i,j}^1 := \min(\gamma_{n,i,j}^1, \gamma_{n,j,i}^1)$  and set:

$$(11) \quad \bar{IC}_{n,i,j}^1 := \begin{cases} IC_{n,i,j}^1 & \text{if } \gamma_{n,i,j}^1 \leq \gamma_{n,j,i}^1 \\ \{c_{n,i,j,s}^1 | 1 \leq s \leq \gamma_{n,j,i}^1\} & \text{if } \gamma_{n,i,j}^1 > \gamma_{n,j,i}^1 \text{ and } i > j \\ \{c_{n,i,j,t+s}^1 | 1 \leq s \leq \gamma_{n,j,i}^1\} & \text{where } t = \gamma_{n,i,j}^1 - \gamma_{n,j,i}^1 \text{ otherwise.} \end{cases}$$

In the second or third case, let  $IC_{n,i,j}^2 := IC_{n,i,j}^1 \setminus \overline{IC}_{n,i,j}^1$ .

**We now invoke Definition 3 with  $d = 2$  and  $U_n = \{(i, j) | 0 \leq i, j \leq n, i \neq j\}$  and with  $X_{n,i,j} = \overline{IC}_{n,i,j}^1$ .** This defines  $\text{RI}\overline{C}^1$ ,  $\text{cd}_{\text{RI}\overline{C}^1}$ ,  $\text{ER}\overline{IC}^1$ . We use  $\overline{\gamma}^1$  to denote  $\text{cd}_{\text{RI}\overline{C}^1}$ . The notation for the increasing enumerations will be  $\overline{c}_{n,i,j,s}^1$ .

**Definition 10.** For  $i < n$ , we set:

$$IA_{n,i}^2 := \bigsqcup_{0 \leq i, j < n, i \neq j} IC_{n,i,j}^2 \text{ and } IB_{n,i}^2 := \bigsqcup_{0 \leq i, j < n, i \neq j} IC_{n,j,i}^2.$$

We also set  $\alpha_{n,i}^2 := |IA_{n,i}^2|$  and  $\beta_{n,i}^2 := |IB_{n,i}^2|$ .

**We now invoke Definition 3 with  $d = 1$  and  $U_n = \{0, \dots, n\}$  and with  $X_{n,i} = IA_{n,i}^2$  or  $X_{n,i} = IB_{n,i}^2$ .** This defines  $\text{RIA}^2$ ,  $\text{RIB}^2$ ,  $\text{cd}_{\text{RIA}^2}$ ,  $\text{cd}_{\text{RIB}^2}$ ,  $\text{ERIA}^2$ ,  $\text{ERIB}^2$ . We use  $\alpha^2$ ,  $\beta^2$  to denote  $\text{cd}_{\text{RIA}^2}$ ,  $\text{cd}_{\text{RIB}^2}$ , respectively. The notation for the increasing enumerations will be  $a_{n,i,s}^1$ ,  $b_{n,i,s}^1$ .

**Proposition 5.** For  $i < n$ ,  $\alpha_{n,i}^2 = \beta_{n,i}^2$ .

*Proof.* We note first that

$$IA_{n,i}^2 = IA_{n,i}^1 \setminus \bigsqcup_{0 \leq j < n, j \neq i} \overline{IC}_{n,i,j}^1 \text{ and that } IB_{n,i}^2 = IB_{n,i}^1 \setminus \bigsqcup_{0 \leq j < n, j \neq i} \overline{IC}_{n,j,i}^1.$$

This follows from the definitions of the  $IA_{n,i}^2$ ,  $IB_{n,i}^2$  and the  $\overline{IC}_{n,i,j}^1$ , and Remark 7. But then, since, by construction,  $\overline{\gamma}_{n,i,j}^1 = \overline{\gamma}_{n,j,i}^1$ , for all relevant  $n, i, j$ , we have that

$$\left| \bigsqcup_{0 \leq j < n, j \neq i} \overline{IC}_{n,i,j}^1 \right| = \left| \bigsqcup_{0 \leq j < n, j \neq i} \overline{IC}_{n,j,i}^1 \right|.$$

Finally, by construction,  $|A_{n,i}^1| = |B_{n,i}^1|$ . It then clearly follows that  $\alpha_{n,i}^2 = \beta_{n,i}^2$ .  $\square$

We can now complete the construction of the  $H_n$ . Proposition 5 makes it clear that the third case of Equation (12), below, will provide a coherent definition and that the  $H_n$  we define there are admissible permutations of  $\{0, \dots, 2^n - 1\}$  with the additional property of  $G_n$ .

**Definition 11.**  $H_n$  is the permutation of  $\{0, \dots, 2^n - 1\}$  defined as follows. If  $0 \leq k < 2^n$ , let  $i = \text{IStep}(n, k)$ ,  $j = \text{Weight}(k)$ . Then:

$$(12) \quad H_n(k) := \begin{cases} k & \text{if } j = i \\ \overline{c}_{n,i,j,s}^1 & \text{where } s = \overline{\gamma}_n^1(i, j, k) \text{ if } k \in \overline{IC}_{n,i,j}^1 \\ b_{n,i,s}^2 & \text{where } s = \alpha_n^2(i, k), \text{ otherwise.} \end{cases}$$

Also (as usual), let:  $H : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$  to be the natural encoding of the sequence  $\{H_n\}$  of admissible permutations.

With reference to the discussion in the final paragraph of (3.5), related to the form of the lower bound expression, we should note here, that even for  $G$ , the situation is somewhat more complicated: it may fail to be true that  $G_n(n) = 2^{n-1}$  (or, in the notation of the final paragraph of (3.5), that  $k(n) = n$ ): this will happen exactly if  $n$  is a power of 2, since then  $\text{Weight}(n) = 1 = \text{IStep}(n, n)$  and so  $G_n(n) = n \neq 2^n$ . In this case, however, we'll have that  $G_n(n-1) = 2^{n-1}$ . This is the basis for Equation (13), below, which is the analogue for  $G$  of Equation (8). We have not carried out a similar analysis of the  $k(n)$  function for  $H$ , and so, in the proof of Theorem 3, in (4.2), we content ourselves with the general lower bound expression given by Equation (6). Similar issues represent similar (but even worse) obstacles to obtaining an analogue of Corollary 4 for  $G$  or  $H$ .

4.2. **Theorem 3.** The analogue of Theorem 2 for the functions  $G$  and  $H$  is provided by Theorem 3. The lower bound statement argument divides, as just discussed, but things rejoin for the proof that  $G$  and  $H$  are P-TIME. Proposition 6 is the main technical tool; it incorporates the contributions of Proposition 4, Lemma 2, Lemma 3 and Corollary 3 in the proof of Theorem 2.

**Proposition 6.** *Each of the following relations is both P-TIME decidable and tame:*  
 $RIA^1$ ,  $RIA^1$ ,  $RIC^1$ ,  $RIC^1$ ,  $RIA^2$ ,  $RIB^2$ . *Also, all of the case conditions of Equations (10) and (12) are P-TIME decidable.*

*Proof.* For each of the listed relations, the hypothesis of item 6. of Remark 3 clearly holds, and so it will suffice to establish tameness. We weave our way through the statements to be proved in the following order. First, the P-TIME decidability of the case condition of Equation (10), then the tameness of  $RIA^1$ ,  $RIB^1$ ,  $RIC^1$ , then the P-TIME decidability of the second case condition of Equation (12) and finally, the tameness of  $RIC^1$ ,  $RIA^2$  and  $RIB^2$ . Throughout the proof we will have  $x \in \mathbb{Z}^+$  with  $x < 2^n$ .

For the case condition of Equation (10) (and the first case condition of Equation (12)), our starting point is Proposition 4, itself. The case condition is just whether  $IStep(n, k) = Weight(k)$ : if so, then it is the first case of Equations (10), (12) of Definitions 7, 11 that applies:  $G(n, k) = H(n, k) = k$ . It follows from Proposition 4 that the relation expressed by the last displayed equation is P-TIME decidable.

For the tameness of  $RIA^1$ , note that for each  $(n, i)$ ,  $IA_{n,i}^1 = IA_{n,i} \setminus (IA_{n,i} \cap IB_{n,i})$ . Recall that  $\beta(n, i, x) - \beta(n, i, SBC(n, i) - 1)$  computes  $|\{m \in IB_{n,i} | SBC(n, i) \leq m \leq x\}|$ . It follows that  $\alpha^1(n, i, x) = \alpha(n, i, x) + \beta(n, i, SBC(n, i) - 1) - \beta(n, i, x)$ . Similarly,  $IB_{n,i}^1 = IB_{n,i} \setminus [SBC(n, i), SBC(n, i + 1))$ . Thus,  $\beta^1(n, i, x) = \beta(n, i, x) - \alpha(n, i, x)$  and so  $\alpha^1$  and  $\beta^1$  are both P-TIME. Therefore,  $RIA^1$ ,  $RIB^1$  are both tame.

For the tameness of  $RIC^1$ , just note that  $IC_{n,i,j}^1 = \{m \in IB_{n,j}^1 | SBC(n, i) \leq m < SBC(n, i + 1)\}$ . It follows that if  $x < SBC(n, i)$  then  $\gamma^1(n, i, j, x) = 0$ , and if  $SBC(n, i + 1) - 1 \leq x < 2^n$  then  $\gamma^1(n, i, j, x) = \beta^1(n, j, SBC(n, i + 1) - 1) - \beta^1(n, j, SBC(n, i) - 1)$ . Finally, if  $SBC(n, i) \leq x < SBC(n, i + 1) - 1$ , then  $\gamma^1(n, i, j, x) = \beta^1(n, j, x) - \beta^1(n, j, SBC(n, i) - 1)$ . Thus,  $\gamma^1$  is P-TIME and so  $RIC^1$  is tame. Note that by Lemmas 2 and 3, we have that  $ERIC^1$  is P-TIME, i.e., for all relevant  $(n, i, j)$  and all  $s$  with  $1 \leq s \leq \gamma_{n,i,j}^1$ ,  $c_{n,i,j,s}^1$  is a P-TIME function of  $(n, i, j, s)$ .

For the tameness of  $RIC^1$ , note that if  $\gamma_{n,i,j}^1 \leq \gamma_{n,j,i}^1$ , then  $\bar{\gamma}^1(n, i, j, x) = \gamma^1(n, i, j, x)$ . If  $\gamma_{n,i,j}^1 > \gamma_{n,j,i}^1$  and  $i > j$ , let  $s = \gamma_{n,j,i}^1$ . If  $x \leq c_{n,i,j,s}^1$ , then  $\bar{\gamma}^1(n, i, j, x) = \gamma^1(n, i, j, x)$ , while if  $c_{n,i,j,s}^1 < x < 2^n$ , then  $\bar{\gamma}^1(n, i, j, x) = s$ . Finally, if  $\gamma_{n,i,j}^1 > \gamma_{n,j,i}^1$  and  $i < j$ , let  $t = \gamma_{n,i,j}^1 - \gamma_{n,j,i}^1$ . If  $x < c_{n,i,j,t+1}^1$ , then  $\bar{\gamma}^1(n, i, j, x) = 0$ , while if  $c_{n,i,j,t+1}^1 \leq x < 2^n$ , then  $\bar{\gamma}^1(n, i, j, x) = \gamma^1(n, i, j, x) - t$ . Thus,  $\bar{\gamma}^1$  is P-TIME, and so  $RIC^1$  is tame, and therefore is P-TIME decidable. We mention this explicitly only because it is exactly the second case condition of Equation (12).

Finally, we show that  $RIA^2$  and  $RIB^2$  are tame. For  $RIA^2$ , if  $0 < i \leq n$ , note:

$$IA_{n,i}^2 = IA_{n,i}^1 \setminus \bigsqcup_{1 \leq j \leq n, j \neq i} IC_{n,i,j}^1.$$

If  $x < SBC(n, i)$ , then  $\alpha^2(n, i, x) = 0$ ; otherwise:

$$\alpha^2(n, i, x) = \alpha^1(n, i, x) - \sum_{1 \leq j \leq n, j \neq i} \bar{\gamma}^1(n, i, j, x),$$

and so  $RIA^2$  is tame. For  $RIB^2$ , we have the analogous observation: for  $0 < i \leq n$

$$IB_{n,i}^2 = IB_{n,i}^1 \setminus \bigsqcup_{1 \leq j \leq n, j \neq i} IC_{n,j,i}^1.$$

Then,  $\beta^2(n, i, x) = \beta^1(n, i, x) - \sum_{1 \leq j, IStep(n, x), j \neq i} \bar{\gamma}^1(n, j, i, x)$ , so  $RIB^2$  is tame.  $\square$

**Theorem 3.** *Each of  $G$ ,  $H$  is P-TIME and is simply computed in terms of SBC.*

*Proof.* As already indicated, we do not attempt to improve on Equation (6) for the lower bound statement for  $H$ . For  $G$ , however, we do note that  $\text{IStep}(n, 2^{n-1}) = \lfloor (n+1)/2 \rfloor > 1$ . Thus,  $2^{n-1}$  is the largest element of  $\text{IB}_{n,1}^1$ , and so if  $k = (G_n)^{-1}(2^{n-1})$ , then  $k$  is the largest element of  $\text{IA}_{n,1}^1$ . As noted at the end of (4.1), possibly  $k \neq n$  (if  $n$  is a power of 2), but, if  $k \neq n$ , then  $k = n-1$  (since (1, 2) is the only pair of consecutive 2-powers). Thus, our analogue of Equation (8) for  $G$  is:

$$(13) \quad 2^n = \max(G(n, n), G(n, n-1)) + \max(G(n, n), G(n, n-1)).$$

Turning to the proof that  $G$  and  $H$  are P-TIME, we know, by Proposition 6, that the case conditions are P-TIME decidable, and that in the first case we have  $G(n, k) = H(n, k) = k$ . For each of the remaining cases (case 2, for  $G$  and cases 2, 3, for  $H$ ), we exhibit P-TIME decidable relations involving  $n, k, m$  whose unique solution,  $m$ , is less than  $2^n$ , is P-TIME and is the value of  $G(n, k)$  (resp.  $H(n, k)$ ) as determined by the case in question. This is done in Equations (14), (15), (16).

For readability, we will use  $i$  as an abbreviation for  $\text{IStep}(n, k)$  in each of these equations, and in Equation (15), we will also use  $j$  as an abbreviation for  $\text{Weight}(k)$ , but the relations expressed by these equations really involve only  $n, k, m$ . The P-TIME computability of the unique solutions depends on Proposition 6, and on Lemma 2 (for the P-TIME computability of the relevant enumerating function) and will be established by exhibiting an equation that specifies the computation.

For case 2 of Equation (10), the P-TIME decidable relation is:

$$(14) \quad \beta^1(n, i, m) \chi_{\text{RIB}^1}(n, i, m) = \alpha^1(n, i, k).$$

The P-TIME computability of the unique solution  $m = G(n, k)$  of Equation (14) is established by:

$$\text{if } \text{RIA}^1(n, i, k) \text{ holds, then } G(n, k) = \text{ERIB}^1(n, i, \alpha^1(n, i, k)).$$

For case 2 of Equation (12), the P-TIME decidable relation is:

$$(15) \quad \bar{\gamma}^1(n, j, i, m) \chi_{\text{RIC}^1}(n, j, i, m) = \bar{\gamma}^1(n, i, j, k).$$

The P-TIME computability of the unique solution  $m = H(n, k)$  of Equation (15) is established by:

$$\text{if } \text{RIC}^1(n, i, j, k) \text{ holds, then } H(n, k) = \text{ERIC}^1(n, j, i, \bar{\gamma}^1(n, i, j, k)).$$

Finally, for case 3 of Equation (12), the P-TIME decidable relation is:

$$(16) \quad \beta^2(n, i, m) \chi_{\text{RIB}^2}(n, i, m) = \alpha^2(n, \text{IStep}(n, k), k).$$

Note also that

$$\text{if } \text{RIA}^2(n, i, k) \text{ holds, then } H(n, k) = \text{ERIB}^2(n, i, \alpha^2(n, i, k)).$$

This means that  $H(n, k)$  is the unique solution of Equation (16), and thus is P-TIME.

The argument that each of  $G, H$  is simply computed in terms of SBC is similar to that in Theorem 2, and involves the straightforward verification that all of the functions involved in Equations (14), (15), (16) are simply computed in terms of SBC. This traces back to examining the proof of Proposition 6. Each of  $\alpha^1, \beta^1$  is explicitly and simply computed in terms of  $\alpha, \beta$  and SBC. Next,  $\gamma^1$  is explicitly and simply computed in terms of  $\beta^1$  and SBC. Then,  $\bar{\gamma}^1$  is explicitly and simply computed in terms of  $\gamma^1$ . Next,  $\alpha^2$  is simply and explicitly computed in terms of  $\alpha^1$  and  $\bar{\gamma}^1$ , while  $\beta^2$  is simply and explicitly computed in terms of  $\beta^1, \bar{\gamma}^1$  and  $\text{IStep}$ . Finally,  $\chi_{\text{RIB}^1}, \chi_{\text{RIC}^1}$  and  $\chi_{\text{RIB}^2}$  can then be computed simply in terms of SBC using the second observation in the first paragraph following the proof of Lemma 3.  $\square$

## REFERENCES

- [1] Beame, P. W., Cook, S. A., Hoover, H. J.: Log depth circuits for division and related problems. Siam Journal on Computing 15, 994-1003 (1986).
- [2] Berti, P., Pratelli, L., Rigo, P.: Skorohod representation theorem via disintegrations. Sankhyā: The Indian Journal of Statistics 72-A, 208-220 (2010).
- [3] Berti, P., Pratelli, L., Rigo, P.: A Skorohod representation theorem for uniform distance. Probability Theory and Related Fields 150(1-2), 321-335 (2011).
- [4] Clote, P., Kranakis, E.: Boolean Functions and Computation Models. Springer , Berlin-Heidelberg-New York (2002).
- [5] Dudley, R.M.: Real Analysis and Probability. Cambridge U. Press, Cambridge (1989).
- [6] Hesse, W., Allender, E., Barrington, D. A. M: Uniform constant-depth threshold circuits for division and iterated multiplication. Journal of Computer and System Sciences 65, 695-716 (2002).
- [7] Khintchine, A.: Über dyadische brüche. Math. Zeit. 18, 109-116 (1923).
- [8] Kolmogoroff, A.: Über das gesetz des iterierten logarithmus. Math. Ann.101, 126-135 (1929).
- [9] The On-Line Encyclopedia of Integer Sequences, published electronically at <http://oeis.org>.
- [10] Papadimitriou, C. H.: Computational Complexity. Addison-Wesley, Reading (1994).
- [11] Skorokhod, A. V.: Limit theorems for stochastic processes. Theory of Probability and its Applications 1, 261-290 (1956).
- [12] Skyers, M.: A tale of two sequences: a story of convergence, weak and almost sure. Dissertation, Lehigh University (2012).

DEPARTMENT OF MATHEMATICS, LEHIGH UNIVERSITY, 14 EAST PACKER AVENUE, BETHLEHEM, PA 18015  
*E-mail address:* `vd00@lehigh.edu`

DEPARTMENT OF MATHEMATICS, LEHIGH UNIVERSITY, 14 EAST PACKER AVENUE, BETHLEHEM, PA 18015  
*E-mail address:* `marinaskyers@gmail.com`

DEPARTMENT OF MATHEMATICS, LEHIGH UNIVERSITY, 14 EAST PACKER AVENUE, BETHLEHEM, PA 18015  
*E-mail address, Corresponding author:* `ljs4@lehigh.edu`